Elektrotechnik & Informationstechnik (2016) 133/7: 319–323. DOI 10.1007/s00502-016-0427-5

IoT als Herausforderung für die Informationssicherheit

I. Schaumüller-Bichl, A. Kolberger

Sowohl Hersteller als auch die ganze Gesellschaft stehen durch das „Internet der Dinge" (Internet of Things, IoT) vor neuen Herausforderungen. Neue Angriffsziele entstehen, und die klassischen Grundanforderungen der Informationssicherheit ändern sich. Der Einsatz neuartiger Technologien in Kombination mit einem widerstandsfähigen Systemdesign und angemessenem Informationssicherheitsmanagement sind erforderlich, um diesen Anforderungen gerecht zu werden.

Schlüsselwörter: Informationssicherheit; Internet der Dinge; Risikoanalyse; Risikomanagement; Physically Unclonable Functions (PUFs); Common Criteria

IoT as a challenge in information security.

Both, manufacturers and the whole society face new challenges due to the upcoming of the "Internet of Things" (IoT). New attack targets arise and typical basic requirements for information security change. The application of new technologies in combination with resilient system design and appropriate information security management are essential in order to address these requirements.

Keywords: Information security; Internet of Things (IoT); Risk analysis; Risk management; Physically unclonable functions (PUFs); Common criteria

Online publiziert am 26. Oktober 2016

1. Einführung

Die Vernetzung unterschiedlichster Komponenten im „Internet of Things" (IoT) eröffnet neue Wege und Möglichkeiten, um Aufgaben zu erleichtern oder effizienter und effektiver zu gestalten. Sie tragen zur Steigerung der Lebensqualität bei oder stellen gar lebenswichtige Funktionalitäten bereit. Diese Chancen bergen aber auch gleichzeitig Risiken, denen adäquat zu begegnen ist. Hier stellen insbesondere die Komplexität, Diversität und Schnelllebigkeit des IoT neue Herausforderungen an die Informationssicherheit.

In diesem Artikel werden die besonderen Eigenschaften des IoT diskutiert und die wichtigsten Aspekte angesprochen, die beim Risikomanagement derartiger Netze zu berücksichtigen sind. Zudem werden neue Technologien für den kostengünstigen Einsatz in Sicherheitsanwendungen beschrieben.

2. Herausforderungen für die Sicherheit im IoT

Vereinfacht gesagt besteht das „Internet der Dinge" aus drei Bereichen:

- den „Dingen", also den Komponenten, die miteinander verbunden werden; dies können Computer, spezielle Geräte, Sensoren oder auch Menschen sein
- den Netzwerken, die diese „Dinge" verbinden
- den Computern und Rechenzentren, in denen die Daten verarbeitet und gespeichert werden

Aus Sicherheitssicht bedeutet das, dass auch im IoT alle „klassischen" Sicherheitsmechanismen gegeben sein müssen: IT-Sicherheit zum Schutz der Komponenten, Kommunikations- bzw. Netzwerksicherheit zum Schutz der Daten bei der Übertragung und Rechenzentrumssicherheit und Cloud Security zum Schutz der Verarbeitung der Daten. Dazu kommen noch Anforderungen aus dem Datenschutz und der physischen Sicherheit. Die klassischen Grundanforderungen der Informationssicherheit, nämlich Vertraulichkeit, Integrität und Verfügbarkeit sind auch im IoT gegeben, auch weitere Anforderungen wie Authentizität, Non Repudiation und Privacy können bestehen.

Darüber hinaus gibt es jedoch im IoT eine ganze Reihe neuer Herausforderungen, es gibt neue Angriffsmöglichkeiten und neue Angriffsziele.

Die Geräte sind „always on", können daher jederzeit, von jedem Ort und an jedem Ort angegriffen werden. Dabei stellen vor allem die Gewährleistung der Verfügbarkeit und der Schutz der Privatsphäre große Herausforderungen dar. Die Schnittstelle zur „realen Welt" verschwimmt in den sog. Cyber Physical Systems, Komponenten, die bisher für sich alleine eingesetzt wurden, können nun vernetzt werden.

Im Folgenden werden die wichtigsten Herausforderungen an die Informationssicherheit im IoT diskutiert.

2.1 Komplexität und Diversität

Schon die Anzahl der Komponenten, die im Internet der Dinge miteinander vernetzt werden, stellt eine Herausforderung dar. Man rechnet beispielsweise damit, dass 2020 eine viertel Milliarde Fahrzeuge[1] miteinander verbunden sein werden. Der Adressraum von IPv6 umfasst 2^{128} IP-Adressen, das entspricht einer Anzahl von

[1] http://www.gartner.com/newsroom/id/2970017 (Zugriff: 29.8.2016).

Schaumüller-Bichl, Ingrid, Information Security Compliance Center (ISCC), FH OÖ Studienbetriebs GmbH, Hafenstraße 47-51 (Techcenter), 4020 Linz, Österreich (E-Mail: ingrid.schaumueller-bichl@fh-ooe.at); **Kolberger, Andrea,** Information Security Compliance Center (ISCC), FH OÖ Studienbetriebs GmbH, Hafenstraße 47-51 (Techcenter), 4020 Linz, Österreich

340 Sextillionen (3.4×10^{38}) unterschiedlichen Adressen. Theoretisch können damit auf absehbare Zeit alle auch noch so winzigen „smarten Dinge" mit einer eigenen IP-Adresse ausgestattet werden [3, S.105].

Eine alte Grundregel der (IT-)Sicherheit besagt, dass „eine Kette nur so stark ist wie ihr schwächstes Glied". Dies gilt im Prinzip natürlich auch für das IoT, d. h. alle Komponenten, Netzwerkverbindungen und insbesondere die zentrale Verarbeitung müssen bestmöglich abgesichert werden. Allerdings wird es gerade auch im IoT notwendig sein, die Fehleranfälligkeit des Gesamtsystems möglichst gering zu halten und die Systeme möglichst widerstandsfähig zu bauen. Zuverlässigkeit, Resilience und Business Continuity werden zentrale Herausforderungen für eine sichere Anwendung des IoT darstellen, Single Points of Failure und Single Points of Attack sind bereits im Systemdesign zu vermeiden, die Systemarchitektur muss also möglichst resilient sein.

Neben der Anzahl der Komponenten stellt auch die Art der Komponenten neue Herausforderungen. Während in klassischen IT-Netzwerken vorwiegend Geräte miteinander kommunizieren, für die mittlerweile bewährte Sicherheitsmechanismen, wie etwa Firewalls, Backups, Berechtigungssysteme und starke Authentisierungsverfahren existieren, kommen im IoT viele weitere Komponenten zum Einsatz, wie etwa spezielle Devices aus dem medizinischen Bereich, der Haussteuerung, Smart Meter, Wearables oder auch einfache Sensoren. Viele dieser Komponenten wurden nicht mit dem Schwerpunkt auf IT-Sicherheit entwickelt und stellen nur wenige oder keine Sicherheitsfunktionen zur Verfügung. Daraus resultiert ein Netzwerk mit einer Vielzahl von potentiell unbekannten Schwachstellen, deren Auswirkungen und Folgen derzeit schwer abzuschätzen sind.

2.2 Verfügbarkeit und Stabilität

IoT-Anwendungen sind grundsätzlich den gleichen Gefährdungen ausgesetzt wie „klassische" Internetanwendungen, also etwa DDoS-Angriffen, oder Malware und müssen auch gegen solche geschützt werden. Dies gilt in besonderem Maße für Anwendungen, in denen Hochverfügbarkeit gefordert ist, etwa in manchen medizinischen Anwendungen oder in der Steuerung von kritischen Infrastrukturen. Darüber hinaus besteht die Gefahr, dass IoT-Komponenten oder IoT-Anwendungen die Verfügbarkeit anderer Systeme beeinflussen. Als Beispiel kann hier die Stabilität von Stromversorgungsnetzen[2], also das Gleichgewicht zwischen Stromerzeugung und Stromverbrauch, angeführt werden. Durch den Einsatz von intelligenten Stromzählern, den sogenannten Smart Metern, entstehen komplexe Netzwerke mit einer großen Anzahl an Einzelgeräten. Findet schlagartig ein großflächiger Ausfall der Smart Meter Komponenten statt und die betroffenen Haushalte und Unternehmen können keinen Strom vom Versorgungssystem beziehen, so bereitet der Stromausfall nicht nur jedem einzelnen Betroffenen Unannehmlichkeiten, der abrupte Ausfall der Energieverbraucher kann auch negative Auswirkungen auf die Netzfrequenz und folglich auf die Stabilität sowie Verfügbarkeit des Übertragungsnetzes oder sogar auf überregionale Stromversorgungsnetze haben (Kaskadeneffekt)[3]. Wie schnell es zu weitreichenden Auswirkungen kommen kann, zeigt ein Vorfall aus dem Jahr 2006. Bei der Überstellung des Kreuzfahrtschiffes Norwegian Pearl von der Werft ans Meer über die Ems war die geplante Abschaltung von zwei Hochspannungsleitungen erforderlich. Infolge von Planungsfehlern und kurzfristigen Änderungen kam es zu Netzüberlastungen und Instabilitäten, die zu einem bis zu 2-stündigen Stromausfall in großen Teilen West- und Südeuropas führten, von dem ca. 15 Mio. Haushalte betroffen waren[4].

2.3 Beschränkungen bei den Komponenten und Devices

Viele der im IoT neu zum Einsatz kommenden Komponenten haben beschränkte Ressourcen, beispielsweise in Hinblick auf Speicherplatz, Verarbeitungsgeschwindigkeit, Schnittstellen oder Stromversorgung. Oft kommen auch Komponenten, die ursprünglich nicht für sicherheitskritische Anwendungen oder für Umgebungen, in denen keine (IT-spezifische) Gefährdung bestand, entwickelt wurden, zum Einsatz. Beispiele dafür sind etwa medizinische Devices oder Komponenten der Haussteuerung, wie Heizung und elektrische Beleuchtung. Zudem besteht gerade bei Einsatz einer großen Anzahl von Komponenten meist ein starker Kostendruck.

Viele der heute etablierten Sicherheitstechniken haben einen relativ hohen Speicherplatz- und Stromversorgungsbedarf, so dass sie in solchen Komponenten nicht oder nur beschränkt zum Einsatz kommen können. Es besteht daher Bedarf an neuen, ressourcenschonenden Verfahren. Neue Entwicklungen im Bereich der Kryptographie (Leightweight Cryptography), der Speichertechnologien und der Stromversorgung (z. B. Inductive Charging) sind wichtige Voraussetzung für einen flächendeckenden sicheren Einsatz von IoT Devices.

Besonders interessant ist in diesem Zusammenhang die Entwicklung der neuen Technologie der Physically Unclonable Funtions (PUFs), die inhärente physikalische Eigenschaften von Chips verwenden, um ein Device eindeutig zu identifizieren und damit die Entwicklung neuer Authentisierungs- und Verschlüsselungsverfahren ermöglichen. Sie werden in Abschn. 4 näher betrachtet.

2.4 Schatten-IT

Gerade in den letzten Jahren hat man sich bemüht, klare Regeln, Vorgehensweisen und Verantwortlichkeiten für den IT-Bereich in Unternehmen und anderen Organisationen einzuführen und durchzusetzen. Managementprozesse und -systeme etwa für Informationssicherheits-Management (ISMS), Business Continuity Management (BCMS), Risikomanagement und Service Level Management gehören heute zum State-of-the-Art einer ordnungsgemäßen Unternehmensführung in jeder größeren Organisation. Wichtige Basis für die Etablierung derartiger Systeme ist eine genaue Kenntnis der IT-Systeme und Anwendungen sowie eine Definition der Regeln zu ihrer Verwendung. Durch den schleichenden Einsatz von IoT-Komponenten besteht die Gefahr, dass es zur Etablierung einer „Schatten-IT" kommt, d. h., dass beispielsweise Systeme ohne Wissen und Genehmigung der Verantwortlichen mit der Unternehmens-IT verbunden werden, neue, nicht genehmigte Komponenten (z. B. private mobile Geräte) zum Einsatz kommen oder IoT-Anwendungen z. B. in der Haussteuerung undokumentiert über WLANs an die Unternehmens-IT angebunden werden.

Damit können erhebliche neue Risiken für eine Organisation und die Gesellschaft entstehen.

Es wird erforderlich sein, in den Unternehmen klare Security-, Assurance- und IT-Governance-Regeln für die Einbindung von IoT-Komponenten und Anwendungen zu etablieren (s. auch [4, S. 11]).

[2] https://energie-wissen.de/netzstabilitaet (Zugriff: 29.8.2016).

[3] http://futurezone.at/netzpolitik/ein-blackout-in-naher-zukunft-ist-realistisch/24.593.018 (Zugriff: 29.8.2016).

[4] https://www.vde.com/de/fg/ETG/Archiv/Publikationen/Rundbriefe/2007-oeffentlich/mi-1/Technik-Trends/2006-exklusiv/Seiten/Stromausfall-2006-11.aspx (Zugriff: 31.8.2016).

2.5 Fehlende Update-Möglichkeiten

Im „klassischen" IT- und Informationssicherheitsbereich ist es unbestritten, dass regelmäßige Updates eine wesentliche Voraussetzung dafür sind, das Sicherheitsniveau eines Systems aufrecht zu erhalten bzw. zu verbessern. Gleiches gilt nun auch für IoT-Systeme und IoT-Anwendungen. Allerdings besteht hier das Problem, dass viele Komponenten, insbesondere Low-Cost-Komponenten, nur über beschränkte oder sogar über keine Update-Möglichkeiten verfügen. Besonderes Augenmerk ist auf Systeme mit sehr langen Lebenszyklen zu richten, hier besteht die Gefahr, dass zugunsten der Verfügbarkeit und Stabilität auf Updates verzichtet wird. So sind beispielsweise heute noch ICS-Systeme (Industrial Control Systems) auf der Basis von Windows XP im Einsatz, obwohl der Hersteller die Wartung eingestellt hat und seit April 2014 keine Patches mehr verfügbar sind.

2.6 Privacy

Eine besondere Herausforderung in IoT-Anwendungen stellt der Schutz der Privatsphäre und der personenbezogenen Daten dar. Schon im täglichen Leben und in der klassischen IT sind sich Benutzer oft nicht bewusst, wie viel von ihren persönlichen Daten sie unbewusst preisgeben. Erst im August 2016 warnte EU-Wettbewerbskommissarin Margrethe Vestager Verbraucher vor Bonus- oder Rabattkarten, mit denen eine Vielzahl von persönlichen Daten und Einkaufgewohnheiten bekanntgegeben würden.[5] Auch in sozialen Netzwerken setzt sich erst langsam ein Datenschutzbewusstsein der Benutzer durch, und damit auch die Erkenntnis, dass nicht jedes private Ereignis mit „Freunden" auf der ganzen Welt geteilt werden muss.

Das Internet der Dinge stellt nun nochmals neue Herausforderungen an die Anwender. Neue Technologien, wie etwa Wearables, Location Based Services und vernetzte medizinische Devices oder einfach nur Apps auf den bereits zum Alltag gehörenden Smartphones geben eine erhebliche Menge an persönlichen Informationen preis. Für den Benutzer oft gar nicht erkennbar werden nun auch medizinische oder biologische Messdaten (beispielsweise in Fitness-Apps), Standortdaten oder Verhaltensdaten weitergegeben.

Aber auch wenn sich Benutzer der potentiellen Risiken bewusst sind, ist eine Durchsetzung der Privacy-Anforderungen nicht einfach. Viele Anwendungen fordern die Zustimmung der Benutzer zur Verwendung ihrer persönlichen Daten, entweder, weil sie tatsächlich benötigt werden (z. B. bei Location Based Services), oft aber auch aus nicht nachvollziehbaren Gründen.

Der zunehmende Einsatz von IoT-Anwendungen wird diese Problematik verstärken. Die heute etablierten Techniken, wie Meldepflichten, Zustimmung und Datensparsamkeit, können nicht eins zu eins in das IoT umgesetzt werden. Es wird neue technische Verfahren, wie etwa Privacy Enhancing Techniques (PETs) für das IoT, aber auch organisatorische und rechtliche Konstrukte sowie ein neues Datenschutzbewusstsein der Betroffenen brauchen, damit wir im Zeitalter des Internets der Dinge nicht vollkommen zu „gläsernen Menschen" werden.

3. Sicherheitsmanagement

Das Internet der Dinge braucht neue Sicherheitskonzepte, die der Komplexität der Netze und der Anwendungen Rechnung tragen, aber auch Vorgaben und Prozesse, die es im Falle eines Fehlers oder eines Angriffes ermöglichen, das System möglichst störungsfrei, ohne Datenlecks und mit geringstmöglichen Auswirkungen auf anderen Systemen weiter zu betreiben.

Dazu bedarf es eines ausgereiften Risiko- und Business Continuity Managements.

3.1 Neue Anforderungen an die Risikoanalyse

Herkömmliche Methoden zur Risikoanalyse, also die Ermittlung von Bedrohungen und Schwachstellen sowie die Bewertung der Eintrittswahrscheinlichkeiten und der Schadenshöhen, können bereits in kleineren Systemen sehr aufwendig werden. Mit zunehmender Komplexität durch die Vernetzung von Systemen entstehen neue Anforderungen an die Risikoanalyse [7].

Ein wesentlicher Unterschied zu normalen IT-Systemen liegt in der großen Anzahl und der Diversität der Komponenten im IoT. Das System ändert sich meist sehr rasch und ist äußerst dynamisch, neue Einzelkomponenten werden eingebunden bzw. entfernt oder werden an anderen Stellen vernetzt. Außerdem müssen in Hinblick auf das Gesamtsystem die korrekte Konfiguration sowie die gegenseitige Abhängigkeit der einzelnen Komponenten bekannt sein. Jede Änderung in der Infrastruktur oder Konfiguration birgt aber potentielle Bedrohungen und Schwachstellen und somit auch neue Risiken in sich. In der Praxis wird es oftmals nicht mehr möglich sein, Risikoanalysen, die aufgrund von Änderungen am System eigentlich erforderlich wären, zeitnah durchzuführen. Daher sind zusätzliche Maßnahmen im Systemdesign (Security/Privacy by Design) und im Risiko- bzw. Sicherheitsmanagement erforderlich.

Risiken in herkömmlichen IT-Systemen werden vorwiegend hinsichtlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (CIA – Confidentiality, Integrity, Availability) bewertet. Aufgrund der Erweiterung der Anwendungsbereiche durch den Einsatz von IoT-Komponenten kann es erforderlich sein, weitere Schutzziele, wie Zuverlässigkeit, Authentizität, Privacy, Non Repudiation oder Betriebssicherheit, zu berücksichtigen, die aber möglicherweise auch miteinander in Konflikt stehen.

Einen wichtigen Aspekt stellt auch die wesentlich stärkere Abhängigkeit zwischen den einzelnen Komponenten im IoT dar. So kann beispielsweise eine scheinbar harmlose Funktionalität in einer kleinen, für sich betrachtet unkritischen, Komponente negativen Einfluss auf die Verfügbarkeit oder den Betrieb von wichtigen Komponenten bzw. das Gesamtsystem haben. Als Beispiel sei ein Vorfall von Mai 2013 angeführt, bei dem Österreich knapp einem großflächigen Stromausfall entkommen ist[6]. Eine grundsätzlich harmlose Zählerabfrage aus dem deutschen Erdgasnetz erging „an alle", die Datenflut aufgrund der Antworten legte regional das europäische Steuerungssystem für Stunden lahm. Keine Erfahrungswerte zu den Auswirkungen von Fehlfunktionen liegen jedoch für zukünftige Anwendungsgebiete vor, wie z. B. beim vollautonomen Fahren, das durch die Vernetzung zahlreicher Sensoren ein Auto beispielsweise „um die Ecke sehen lässt".

Eine weitere Herausforderung besteht darin, dass Risikoanalysen im Bereich der Informationssicherheit (Information Security Risk Analysis, ISRA) üblicherweise eine Vielzahl von Einzelrisiken liefern, die für sich gesondert behandelt werden. Gerade in hochkomplexen Systemen, wie es IoT-Anwendungen häufig sind, wird es wichtig sein, abzuschätzen, welches Gesamtrisiko für ein Unternehmen oder für die Gesellschaft aus der Vielzahl von Einzelrisiken solcher Systeme und Komponenten resultiert (vgl. [7]). Einen interessanten Ansatz zur Risikoaggregation auf Basis eines Graphenkonzeptes gibt etwa [8].

[5] http://www.zeit.de/news/2016-08/07/deutschland-eu-kommissarin-warnt-kunden-vor-rabattkarten-07161007 (Zugriff: 29.8.2016).

[6] http://fm4.orf.at/stories/1717900 (Zugriff: 29.8.2016).

In Anbetracht der angeführten Besonderheiten im IoT sind herkömmliche Risikoanalyseverfahren nicht ausreichend. Neue Methoden und Verfahren sind erforderlich, die die Gefährdungen und ihre Auswirkungen (Impacts) in IoT-Systemen und IoT-Anwendungen möglichst realistisch und zeitnah abschätzen.

3.2 Sicherheitsmanagement für organisationsübergreifende IoT-Anwendungen

ISO/IEC 27001 Information Security Management Systems – Requirements [8] gilt heute als der internationale Standard zum Sicherheitsmanagement. Er regelt die Festlegung von Sicherheitszielen und -strategien sowie Verantwortlichkeiten im Bereich der Informationssicherheit einer Organisation und fordert die Einrichtung, Überprüfung und ständige Verbesserung von sicherheitsunterstützenden Prozessen wie Risikoanalyse und Risikomanagement, Incident Handling und Compliance zu vertraglichen und/oder rechtlichen Vorgaben.

Viele dieser Anforderungen gelten gleichermaßen im IoT. Allerdings ist ISO/IEC 27001 für den Einsatz in einzelnen Unternehmen konzipiert, IoT-Anwendungen sind aber oft unternehmensübergreifend.

Es werden daher neue Konzepte für die Einrichtung eines (unternehmensübergreifenden) Sicherheitsmanagements für IoT-Systeme und IoT-Anwendungen erforderlich sein, insbesondere in Umgebungen, die Auswirkungen auf die Gesellschaft oder sogar Gesundheit und Leben haben.

Einen ersten Ansatz für ein organisationsübergreifendes Sicherheitsmanagement gibt ISO/IEC 27010 [8], der Standard für Sicherheitsmanagement zum Informationsaustausch in „information sharing communities", etwa kritischen Infrastrukturen.

Ähnliche Überlegungen werden auch für das IoT notwendig sein, wobei hier besonders die Bereiche Verfügbarkeit, Resilience und physische Sicherheit zu beachten sein werden.

3.3 Business Continuity und Resilience

Im IoT wird es kaum mehr möglich sein, alle Komponenten und Kommunikationsverbindungen adäquat zu schützen. Es sind daher Strategien zu entwickeln, wie mit Betriebsunterbrechungen, Fehlern oder Angriffen umzugehen ist, so dass ein Störfall möglichst geringe Auswirkungen hat und ein System möglichst rasch wieder in den Normalbetrieb kommt. Neben den „klassischen" Business Continuity Betrachtungen, bei denen Strategien für den Krisen- und Katastrophenfall erarbeitet werden, wird im IoT auch die Frage nach der Resilienz von Systemen, also ihrer Widerstandsfähigkeit gegen Störungen, Fehler und Angriffe, eine große Rolle spielen. Redundanzen, virtuelle Systeme und alternative Übertragungstechnologien sind wichtig, um Systeme widerstandsfähiger zu machen.

Des Weiteren sollte bereits beim Design von Systemen darauf geachtet werden, dass „Single Points of Failure" bzw. „Single Points of Attack" vermieden werden, dass die Architektur also so gestaltet ist, dass nicht durch das Brechen eines Teils des Systems alle Daten preisgegeben werden oder die Funktionalität des Gesamtsystems gefährdet ist. Kompromittierte Komponenten und Netze müssen von anderen Systemteilen abgeschottet werden können, damit sie dort isoliert, evaluiert und ev. wiederhergestellt werden können.

3.4 Incident Response und Verantwortlichkeiten

Sollte es zu einem Sicherheitsvorfall kommen, so ist auch bei IoT-Anwendungen klar zu definieren, wie die Meldewege aussehen und wer für welche Aktionen verantwortlich ist. Ansprechpartner, Meldewege und Prozesse sind – gegebenenfalls organisationsübergreifend – festzulegen und bekanntzumachen. Im Consumer-Bereich sind die Endverbraucher über ihre Rechte und Pflichten sowie über Ansprechpartner und Reaktionsmöglichkeiten zu informieren.

4. Technologische Lösungsansätze

Die nächsten Jahre werden voraussichtlich auch eine Reihe neuer technologischer und Lösungsansätze für die genannten Probleme mit sich bringen. Ein in mehrerer Hinsicht vielversprechendes Beispiel dafür stellen die Physically Unclonable Functions (PUFs) dar.

Hierbei handelt es sich um neue kostengünstige HW-Lösungen, die inhärente physikalische Eigenschaften von Elektronikbauteilen nutzen. Bereits im Fertigungsprozess werden diese Parameter ausgelesen und in Form eines digitalen Fingerprints des Integrated Circuits (ICs) – vergleichbar mit dem menschlichen Fingerabdruck – verwendet. Es ist damit nicht mehr erforderlich Schlüssel am Gerät zu speichern, denn das Gerät selbst ist der Schlüssel [6].

Die zugrundeliegende Funktionsweise beruht auf einem Challenge-Response-Verfahren, indem ein PUF-basiertes Gerät eine Challenge erhält und aufgrund seiner physikalischen Eigenschaften eine Response generiert, die ausschließlich von dieser einen PUF-Instanz erzeugt werden kann. Die Response, also der Schlüssel oder das Geheimnis, muss nicht gespeichert werden, sondern wird bei Bedarf erzeugt. Diese neuartigen Sicherheitsfeatures können in zahlreichen Anwendungsgebieten eingesetzt werden, beispielsweise für Authentisierungszwecke oder zur Erzeugung von kryptografischen Schlüsseln. Software kann an ein bestimmtes Device gebunden werden (HW/SW Binding), indem der Code mit einem Secret verschlüsselt wird, das von der PUF-Instanz desselben Gerätes erzeugt wird, auf dem die Software gespeichert wird.

Ein weiterer, in erster Linie wirtschaftlicher Vorteil dieser Technologie besteht darin, dass bestehende Hardware bereits über Eigenschaften von PUFs verfügen kann, beispielsweise das inhärente Verhalten von SRAM-Zellen, wenn sie mit Spannung versorgt werden. Dieses Verhalten kann während der Herstellung nicht beeinflusst werden, ist für jedes Gerät individuell und muss nicht explizit „produziert" werden.

Um das Vertrauen in und die Sicherheit von Produkten und Systemen zu erhöhen, könnten die international anerkannten Common Criteria (CC) angewendet werden [1]. Mit Hilfe der CC können funktionale Sicherheitsanforderungen und Anforderungen an die Vertrauenswürdigkeit von Produkten definiert und evaluiert werden. Damit können Produkte verglichen und Sicherheitsstandards in IoT-Systemen etabliert werden. Schutzprofile (Protection Profiles – PPs) betrachten nicht nur die funktionalen Aspekte, sondern auch Rahmenbedingungen und Annahmen, die zum verlässlichen Einsatz von Produkten erfüllt sein müssen. Diese ganzheitliche Betrachtung kann möglicherweise bereits im Systemdesign und später auch in der Risikoanalyse bzw. dem Risikomanagement hilfreich sein. Die wesentlichen funktionalen und nicht-funktionalen Anforderungen speziell für PUF-basierte Produkte sowie ein Auszug aus einem Draft-Schutzprofil nach den Vorgaben der CC sind in [5] zu finden.

Da PUF-Technologie auf physikalischen Messungen beruht, sind PUF-generierte Responses fehlerbehaftet, sozusagen „noisy", d. h. die Bitfolge einer Response ist nicht immer vollständig ident. Zudem können sich im Laufe der Zeit die Eigenschaften einer PUF-Instanz durch Ageing-Effekte (Umwelteinflüsse, Lebensdauer, Anzahl der Aktivierungen, etc.) verändern. Mit Error Correcting Codes (fehlerkorrigierenden Codes) und Anti-Ageing-Mechanismen kann diesem unerwünschten Nebeneffekt entgegengewirkt werden. Forschungsergebnisse zeigen, dass durch die Implementierung von neuartigen Low-Cost-Algorithmen und Protokollen die Verlässlichkeit von PUF-basierten Modulen gesteigert werden kann [2].

5. Resümee

Das Internet der Dinge bringt aus Sicherheitssicht das Zusammenwachsen unterschiedlicher Disziplinen wie IT-Sicherheit, Informationssicherheit, Zuverlässigkeit, Resilience (Widerstandsfähigkeit),

Datenschutz und IT-Governance. Die bestehenden Risiken müssen ganzheitlich betrachtet werden, in vielen Fällen wird es auch notwendig sein, möglicherweise in Konflikt miteinander stehende Schutzgüter, wie beispielsweise die Verfügbarkeit der Systeme und den Schutz der Privatsphäre, abzuwägen und tragfähige Kompromisse zu finden.

Literatur

1. Common criteria for information technology security evaluation (2012): Part 1: introduction and general model; CCMB-2012-09-001, version 3.1, revision 4. Online access: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf (Zugriff: 29.8.2016).
2. Deutschmann, M., Höberl, M., Petschnigg, Ch., Schaumüller-Bichl, I., Kolberger, A., Mazzoli, M., Heuberger, C. (2014): D3.1 – Hybrid FPGA ASIC prototype, projekt CODES (algorithmic extraction and error correction codes for lightweight security anchors with reconfigurable PUFs). Online access: https://www.technikon.com/download/deliverables/CODES-835932-D31-Hybrid-FPGA-ASIC-prototype-PU.pdf (Zugriff: 29.8.2016)
3. Eckert, C. (2014): IT-Sicherheit. Konzepte – Verfahren – Protokolle 9. Aufl. München: Oldenbourg Wissenschaftsverlag GmbH.
4. ISACA (2015): Internet of things – risk and value considerations (white paper). Online access: http://www.isaca.org/KNOWLEDGE-CENTER/RESEARCH/RESEARCHDELIVERABLES/Pages/internet-of-things-risk-and-value-considerations.aspx (Zugriff: 29.8.2016)
5. Kolberger, A., Schaumüller-Bichl, I., Brunner, V., Deutschmann, M. (2014): Protection profile for PUF-based devices: ICT systems security and privacy protection. In IFIP advances in information and communication technology (Bd. 428, S. 91–98). Berlin: Springer.
6. Kolberger, A., Schaumüller-Bichl, I., Deutschmann, M. (2015): Physically Unclonable Functions (PUFs) als neue Technologie in Sicherheitsanwendungen. In 9. Forschungsforum der Österreichischen Fachhochschulen, Technik/Ingenieurwissenschaften/Informationstechnologie. FFH open access repository. Online access: http://ffhoarep.fh-ooe.at/handle/123456789/353 (Zugriff: 29.8.2016).
7. Schaumüller-Bichl, I., Kolberger, A. (2016): Information Security Risk Analysis in komplexen Systemen – neue Herausforderungen und Lösungsansätze. Lecture notes in informatics (LNI). Bonn: Gesellschaft für Informatik.
8. Schiebeck, S., Latzenhofer, M., Palensky, B., Schauer, S., Quirchmayr, G., Benesch, T., Göllner, J., Meurers, C., Mayr, I. (2015): Implementation of a generic ICT risk model using graph databases. In Proc. SECUWARE 2015 (S. 146–153). Venedig.
9. ISO/IEC (2013): ISO/IEC 27001:2013: information technology – security techniques – information security management systems – requirements. International Standards Organization, International Electrotechnical Committee.
10. ISO/IEC (2015): ISO/IEC 27010:2015: Information technology – security techniques – information security management for inter-sector and inter-organizational communications. International Standards Organization, International Electrotechnical Committee.

Autorinnen

Ingrid Schaumüller-Bichl
studierte Technische Mathematik an der Johannes Kepler Universität Linz und habilitierte sich im Fach Angewandte Informatik an der Universität Klagenfurt. Seit 2006 ist sie Professorin an der FH OÖ, Campus Hagenberg, seit 1. März 2015 Leiterin des neugegründeten Information Security Compliance Centers (ISCC) der FH OÖ Studienbetriebs GmbH. Umfangreiche internationale Forschungs-, Entwicklungs- und Lehrtätigkeit in den Bereichen Sicherheits- und Risikomanagement, Kryptographie, Chipkarten, digitale Signaturen, Sicherheitszertifizierungen und Schutz Kritischer Infrastrukturen. Dr. Schaumüller-Bichl ist weiters Leiterin des Arbeitskreises IT-Sicherheit der OCG, stellvertretende Vorsitzende von IFIP TC11 Security and Privacy Protection in Information Processing Systems und Mitglied der Permanent Stakeholders Group (PSG) der European Union Network and Information Security Agency (ENISA).

Andrea Kolberger
absolvierte den Bachelor- und Master-Studiengang „Sichere Informationssysteme" an der FH OÖ, Campus Hagenberg. Die Abschlussarbeiten legten die Schwerpunkte auf IT Governance (Einführung und Anwendung von COBIT in der Praxis) und sicheres Schlüsselmanagement in kritischer Infrastruktur (im Speziellen für den Energiesektor). Sie ist Mitarbeiterin im Information Security Compliance Center (ISCC) der FH OÖ Studienbetriebs GmbH und führt (Compliance-)Prüfungen in organisatorischen als auch technischen Bereichen von Informationssystemen durch. Darüber hinaus gibt das ISCC auch generelle Best-Practice-Vorgaben und Empfehlungen zur Informationssicherheit, wie etwa zum Aufbau eines Sicherheitsmanagements.