Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Grundseminar

Sascha Waltz

IT-Sicherheit im Internet of Things

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Sascha Waltz

IT-Sicherheit im Internet of Things

Grundseminararbeit eingereicht im Rahmen der Grundseminarprüfung
im Studiengang Master Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Kai von Luck
Zweitgutachter: Prof. Dr. Klaus-Peter Kossakowski

Abgegeben am 14.03.2016

Sascha Waltz

Thema der Arbeit

IT-Sicherheit im Internet of Things

Stichworte

IT-Sicherheit, Internet of Things, IoT, Security, Keyless, Entry, Smart-Home

Kurzzusammenfassung

Auch wenn der Begriff "Internet of Things" schon seit mehr als 15 Jahren besteht, wurde er erst in den letzten Jahren wirklich ausgebaut. Immer mehr Geräte werden miteinander vernetzt, ganze Smart-Home Umgebungen entstehen, all dies ist oftmals über das Internet steuer- oder kontrollierbar. Welche Risiken und Angriffsmöglichkeiten bieten solche Umgebungen? Wie läßt sich ein Mißbrauch verhindern? In meinem Masterthema möchte ich in der Multiagenten-Umgebung des Living Place diesen und weiteren sicherheitsrelevanten Fragestellungen nachgehen und Möglichkeiten entwicklen, die solche Sicherheitslücken verhindern. Ein Hauptaugenmerk wird dabei auf die Keyless-Entry Technologie gelegt werden, die es ermöglicht, ein Schloss ohne einen Schlüssel zu öffnen.

Sascha Waltz

Title of the Paper

IT-Security in the Internet of Things

Keywords

IT-Security, Internet of Things, IoT, Security, Keyless, Entry, Smart-Home

Abstract

Although the term "Internet of Things" has existed for more than 15 years, he has really developed only in recent years. More and more devices are networked together, all the smart home environments arise, all this is often controllable via the Internet or controllable. What risks and attack opportunities such environments? How can we prevent abuse? In my master topic I want to address these and other security-related issues in the multi-agent environment of Living Place and develop ways to prevent such vulnerabilities. A main focus is on the keyless entry technology are placed, which makes it possible without a key to open a lock.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

In diesem Kapitel soll das gewählte Thema und die Motivation dahinter erklärt werden.

1.1 Geschichte des Internet of Things

Die ersten Ankündigungen des "Internet of Things"(IoT) gehen schon bis in die 60er Jahre zurück, so schrieb z. B. Karl Steinbuch schon 1966 in seinem Buch "Die informierte Gesellschaft":

> "Es wird in wenigen Jahrzehnten kaum mehr Industrieprodukte geben, in welche die Computer nicht hinein gewoben sind. " Steinbuch (1966)

Einige Jahre später wurde das Thema schon etwas konkreter und Mark Weiser sprach 1991 in seinem Aufsatz "The Computer of the 21st Century" von Ubiquitous Computing und Smart Homes.[1] Als Erfinder des Begriffs gilt allerdings Kevin Ashton, dieser sprach im Jahr 1999 zum ersten Mal vom Internet of Things.[2] Er beschrieb das IoT als Verknüpfung eindeutig identifizierbarer physischer Objekte (things) mit einer virtuellen Repräsentation in einer Internet-ähnlichen Struktur. Die Bekanntheit des Begriffs wurde weiter voran getrieben, als Ashton im gleichen Jahr mit einigen Anderen die Auto-ID Labs gründete, wo man sich damit befasst, physische Objekte in der virtuellen Realität erkennbar zu machen, damit man mit ihnen auf dieser Ebene interagieren kann, um die Informationslücke zwischen realer und virtueller Welt zu schließen.

[1] vgl. Weiser (1999)
[2] vgl. Ashton (2009)

1.2 Motivation

Seit damals ist das Internet der Dinge stark gewachsen und die Visionen sind nahezu Realität geworden. Überall im Alltag sind Computer integriert und agieren miteinander und auch mit Dingen oder Menschen in ihrer Umgebung, ohne dass man davon Notiz nimmt. In vielen Fällen vereinfachen diese vernetzten Dinge den Alltag in ihrer Umgebung, um dies aber tun zu können, müssen sie Daten sammeln, mit anderen Dingen in ihrer Umgebung kommunizieren und interagieren und ebenfalls Informationen bereitstellen. Hierbei kommt der Sicherheitsaspekt oft zu kurz oder wird womöglich ganz außer acht gelassen.
In Abbildung 1.1 sieht man eine Vision der Firma Libelium, vorgestellt auf dem "Meeting of the Minds – Smart Cities 2.0: What Works Today" im November 2015.

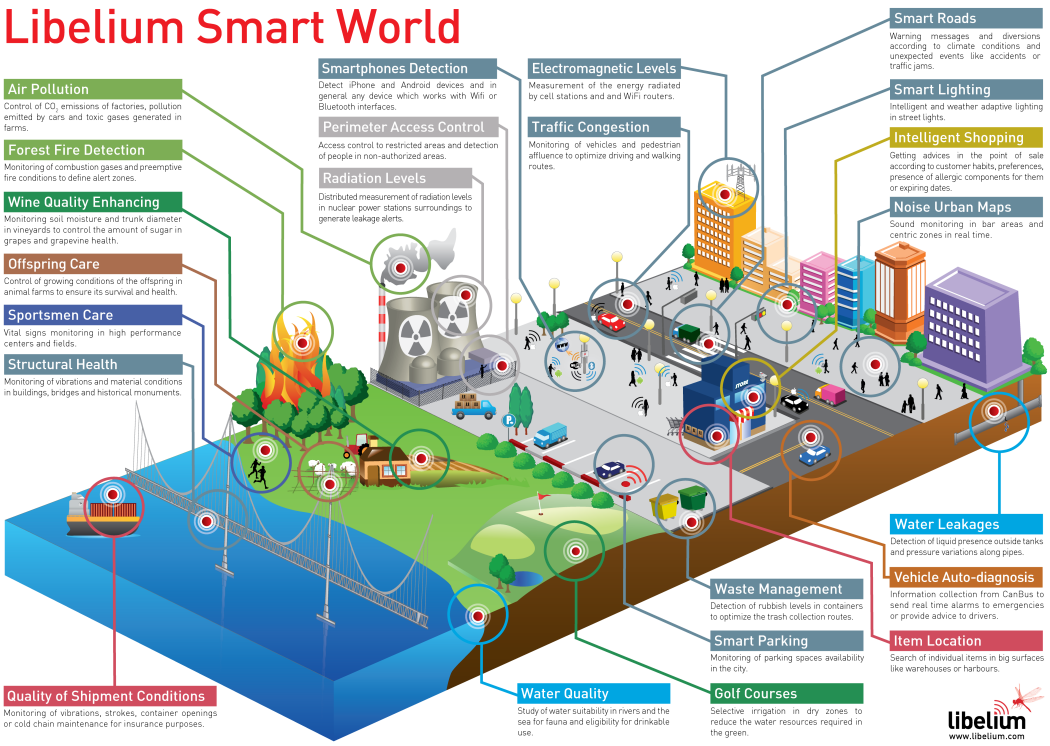

Abbildung 1.1: Libelium Smart World (vgl. Libelium2015)

Diese Grafik zeigt, welche Dinge bis zum Jahr 2020 im Internet of Things vernetzt sein könnten. Einige davon arbeiten heute schon wie angezeigt. Der wachsende Umfang der Dinge, ihre Einsatzbereiche und die (sensiblen) Daten die sie sammeln machen es jedoch unerlässlich, sich auch um den Aspekt Sicherheit Gedanken zu machen. Was genau der Aspekt Sicherheit im Internet of Things bedeutet und wie er differenziert werden sollte, wird in Abschnitt 2.2 behandelt werden.

2 Analyse

In diesem Kapitel soll gezeigt werden, wie der aktuelle Stand der Technik im Bereich des Internet of Things ist, an welchen Stellen geforscht wird und welche Aspekte der IT-Sicherheit in der Vergangenheit und aktuell im IoT aufgetaucht sind.

2.1 Internet of Things

Das Internet of Things (dt. Internet der Dinge) ist, grob zusammen gefasst, ein ständig wachsendes Netzwerk von Sensoren und Aktoren, mit denen der Zustand realer Dinge im Internet bekannt gemacht wird und darauf reagiert werden kann. Neben dem, immer wieder gerne als Beispiel für das IoT gebrachten, Kühlschrank, der eigenständig Lebensmittel nachbestellt, gibt es inzwischen sehr viel mehr Anwendungsbereiche, Abbildung 1.1 zeigt hierfür schon einige Beispiele.
Einen großen Beitrag zum IoT leisten die Auto-ID Labs seit 1999. Diese beschäftigen sich überwiegend mit Radio-Frequency Identification (RFID), Sensor-Netzwerken und neu entstehenden Sensor-Technologien. Viele Firmen nutzen hieraus entstandene Technologien zur Automatisierung von z. B. Fertigungsketten und der Identifizierung von Teilen anhand des elektronischen Produktcodes (EPC).
Durch die immer weiter voranschreitende Entwicklung entwickeln sich auch die Möglichkeiten des IoT immer weiter. Sensoren werden kleiner, leistungsfähiger, langlebiger und zuverlässiger. So lassen sich immer mehr reale Dinge im IoT präsent machen. Die Datensammlung dieser Dinge wird immer weiter automatisiert und sie sammeln diverse Kontextinformationen ihrer Umgebung und stellen diese wiederum anderen Dingen oder auch Entwicklern und Usern zur Verfügung.
Sensoren müssen nicht unbedingt statisch an einem festgelegten Ort installiert werden, an dem sie dann fortan ihren Dienst verrichten. Das Institut für Telematik an der

Universität Karlsruhe hat z. B. im Jahr 1999 schon einige Kaffeebecher mit Rechnertechnologie ausgestattet, die es ermöglicht Kontextinformationen der Tasse abzurufen und mit der Umgebung zu kommunizieren. (vgl. Telecooperation Office (TecO) - Institut für Telematik - Universität Karlsruhe, 1999) Mit Hilfe dieser Technologie ist es möglich die Bewegung der Tasse, bzw. ihres Besitzers in der Umgebung des Forschungslabors zu verfolgen und darauf zu reagieren. Betritt der Besitzer mit seiner Tasse beispielsweise einen Raum, lassen sich die Lampen einschalten. Ein anderes Szenario ist die Umleitung von Anrufen, wenn sich Tasse und Besitzer längere Zeit, etwa für eine Konferenz, in einem Raum aufhalten.

Abbildung 2.1: MediaCup (vgl. Telecooperation Office (TecO) - Institut für Telematik - Universität Karlsruhe, 1999)

Dieses Forschungsprojekt ist ein sehr gutes Beispiel dafür, wie nicht nur Dinge im IoT präsent gemacht werden können, sondern in Verbindung damit auch ihre Benut-

zer. Heutzutage ist diese Verbindung sogar noch einfacher geworden, da nahezu jeder Mensch ein Smartphone bei sich trägt und somit kein extra “Ding“ mehr benötigt wird.
In Abbildung 2.2 zeigt eine Grafik, die vom National Intelligence Council prognostizierte Entwicklung des Internet of Things bis 2025.

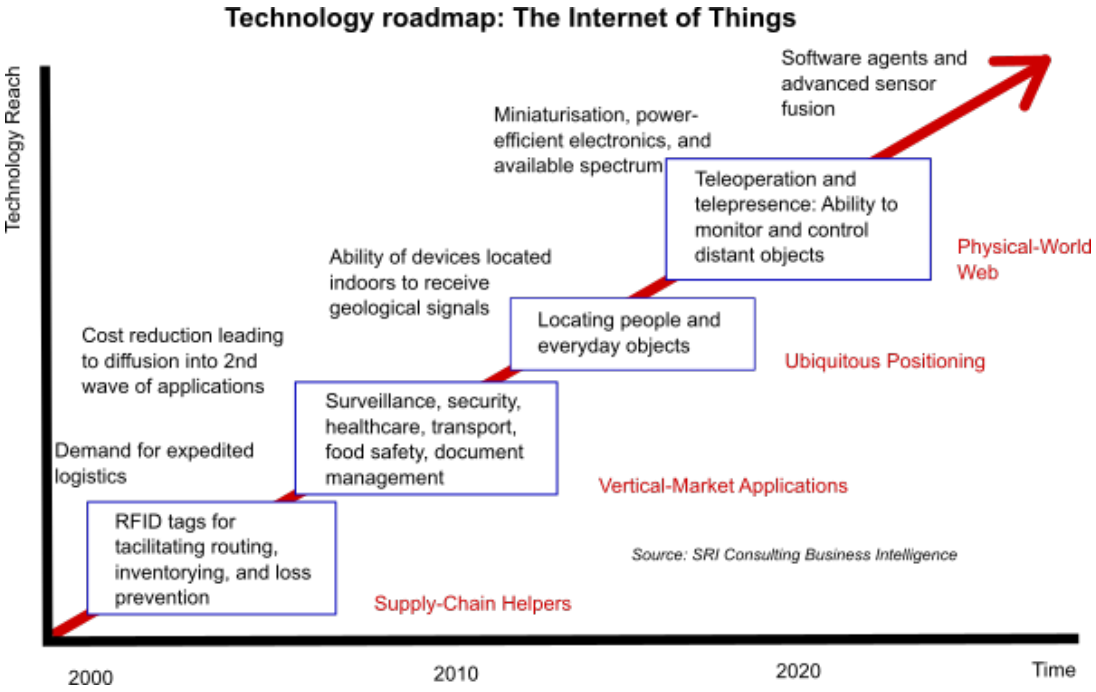

Abbildung 2.2: Technology Roadmap: The Internet of Things (vgl. National Intelligence Council, 2008)

Zur Zeit befinden wir uns im Abschnitt “Locating people and everyday objects“. Der zuvor angesprochene MediaCup war schon ein Beispiel für eine Möglichkeit, die zur Lokalisierung der alltäglichen Objekte genutzt werden kann. Die Entwicklung im Bereich der Lokalisierung von Personen läuft überwiegend über Smartphones, insbesondere wenn es darum geht, die Personen auch zu identifizieren.
Neben der Integration von Sensoren zur Erfassung von Daten der Dinge und ihrer Umgebung hat sich die Definition des IoT dahingehend erweitert, dass auch Aktoren dazugehören. Diese reagieren z. B. auf die von den Sensoren erfassten Daten und

beeinflussen dadurch ihre Umwelt. Bei solchen Systemen spricht man im allgemeinen von “Awareness Technology“, da diese Technologie auf ihr Umfeld reagiert und mit im interagiert.
Im Internet of Things kommen inzwischen diverse verschiedene Technologien zum Einsatz, doch alle haben einige Eigenschaften gemeinsam: Da die Geräte meist sehr lange laufen müssen und sich an Orten befinden, an denen sich nicht unbedingt Menschen aufhalten oder ein Stromanschluss vorhanden ist, müssen die Geräte mit Batterien/Akkus laufen und müssen somit einen sehr geringen Energieverbrauch aufweisen. Viele werden daher so konfiguriert, dass sie nur zu Messungen aktiv werden und sonst im Standby laufen. Des Weiteren müssen die Geräte sehr zuverlässig sein, da ein Ausfall bedeutet, dass ein Gerät repariert oder ausgetauscht werden muss.
Aktuelle Systeme, die im IoT genutzt werden sind Minicomputer wie der Raspberry Pi oder Arduino, welche noch recht viel Storm benötigen. Weitere Systeme, wie “System-on-a-chip (SoC)“, bei dem diverse Funktionen in einem Microprozessor untergebracht werden, oder dem Michigan Micro Mote, CPU, Sensoren und Funkmodul auf der aktuell kleinst möglichen Fläche vereint [1]. Auch in den nächsten Jahren ist zu erwarten, dass die Entwicklung immer weitere Technologien hervorbringt, die immer Leistungsfähiger werden.

2.2 IT-Sicherheit

IT-Sicherheit ist auch im Internet of Things ein wichtiges Thema.

> “IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind. “ BSI - Bundesamt für Sicherheit in der Informationstechnik (2013)

[1] vgl. http://www.eecs.umich.edu/eecs/about/articles/2015/Worlds-Smallest-Computer-Michigan-Micro-Mote.html

Grade im IoT sind Integrität und Verfügbarkeit von Daten sehr wichtig. Wenn die von Dingen gesammelten und bereitgestellten Daten verfälscht wurden oder nicht verfügbar sind, kann das ganze System nicht richtig oder gar nicht funktionieren. Grade manipulierte Daten bergen die Gefahr, dass der Angreifer durch die Manipulation Einfluss auf Systeme nehmen kann, die auf Basis dieser Daten arbeiten. Werden beispielsweise Daten von Rauch- oder Feuermeldern verfälscht, werden u. U. Brandschutzmaßnahmen ausgelöst oder fälschlicher Weise die Feuerwehr alarmiert. Im schlimmsten Fall können durch eine solche Manipulation Menschen zu Schaden kommen.
Der IT-Grundschutz gibt einige Punkte vor, die auch im IoT gelten:

Vertraulichkeit Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Authentizität Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden.

Integrität Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.

Autorisierung Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

Nichtabstreitbarkeit Hierbei liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen

Nichtabstreitbarkeit der Herkunft Es soll einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten.

Nichtabstreitbarkeit des Erhalts Es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten.

Verfügbarkeit Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

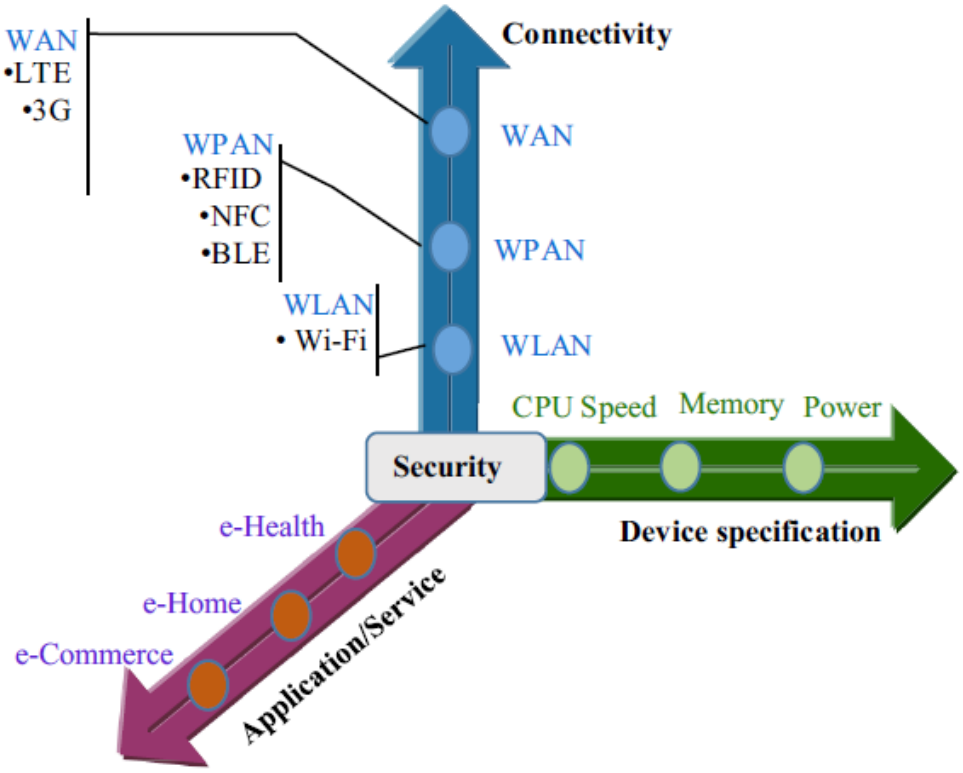

Abbildung 2.3: Security Landscape (vgl. Hossain u. a., 2015)

Die Umsetzung dieser Punkte muss auch oder grade im Internet of Things gewährleistet werden um ein sicheres und zuverlässiges System zu schaffen.
Auf dem “2015 IEEE World Congress on Services“ wurde ein Paper veröffentlicht, das

sich mit Sicherheitsproblemen und -herausforderungen im IoT befasst hat[2]. Die Autoren gehen dabei auf sehr viele verschiedene Schwachstellen und Angriffsmöglichkeiten von IoT-Geräten ein. Anhand der Abbildung 2.3 wird hier aufgezeigt, in welche Parameter im Internet of Things einen Einfluss auf die Sicherheitsaspekte haben können. Die Komplexität der Sicherheit variiert mit jedem Parameter in jeder Dimension der Grafik. Ebenso variieren die Angriffsmöglichkeiten, wie Abbildung 2.4 zeigt. Auf Grund der Beschaffenheit der Dinge im IoT ist es oft schwierig die entsprechenden Sicherheitsmaßnahmen auf dem Gerät zu implementieren ohne das es überlastet wird.

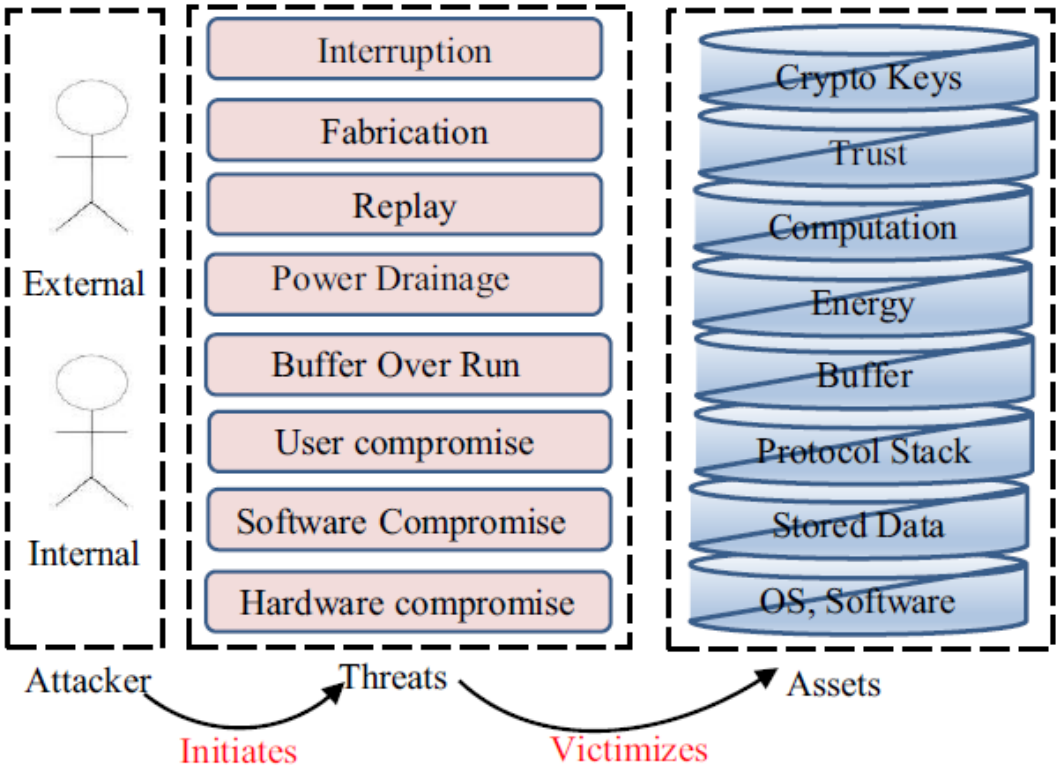

Abbildung 2.4: Consolidated Threat Model (vgl. Hossain u. a., 2015)

Befindet man sich in einem kompletten System von Dingen, wie z. B. einem SmartHome, welches aus diversen "Dingen" besteht, lassen sich einige sicherheitsrelevante

[2] Hossain u. a. (2015)

Aspekte auch systemübergreifend einbauen. In einem solchen SmartHome ist es ebenfalls sehr wichtig, dass einzelne Geräte sicher sind und nicht dazu ausgenutzt werden können, um andere Geräte zu manipulieren. Das System des SmartHomes muss in sich sicher sein, um die Sicherheit nach außen zu gewährleisten.
Hier kommt ebenfalls noch ein weiterer sicherheitsrelevanter Faktor hinzu. Die Keyless-Entry-Technologie wird ebenfalls immer verbreiteter. Sie ermöglicht es, Türen zu öffnen, ohne einen konventionellen Schlüssel zu benötigen. Man nutzt ein weiteres Ding, oft wird das Smartphone oder eine in das Smartphone integrierte Technik genutzt, um sich "auszuweisen", woraufhin das System die Tür öffnet. Ein ähnliches System findet man auch in Autos, insbesondere in Carsharing-Fahrzeugen. Auch hier gibt es wieder diverse Möglichkeiten für einen Angreifer. Er kann ein autorisiertes Smartphone in seinen Besitz bringen, die ID eines autorisiertes Smartphone kopieren oder eine eigene ID in das System einschleusen um sein eigenes Smartphone zu autorisieren. Diese und diverse weitere Möglichkeiten machen es unerlässlich, für ein angemessenes Sicherheitsniveau in SmartHomes und dem Internet of Things zu sorgen.

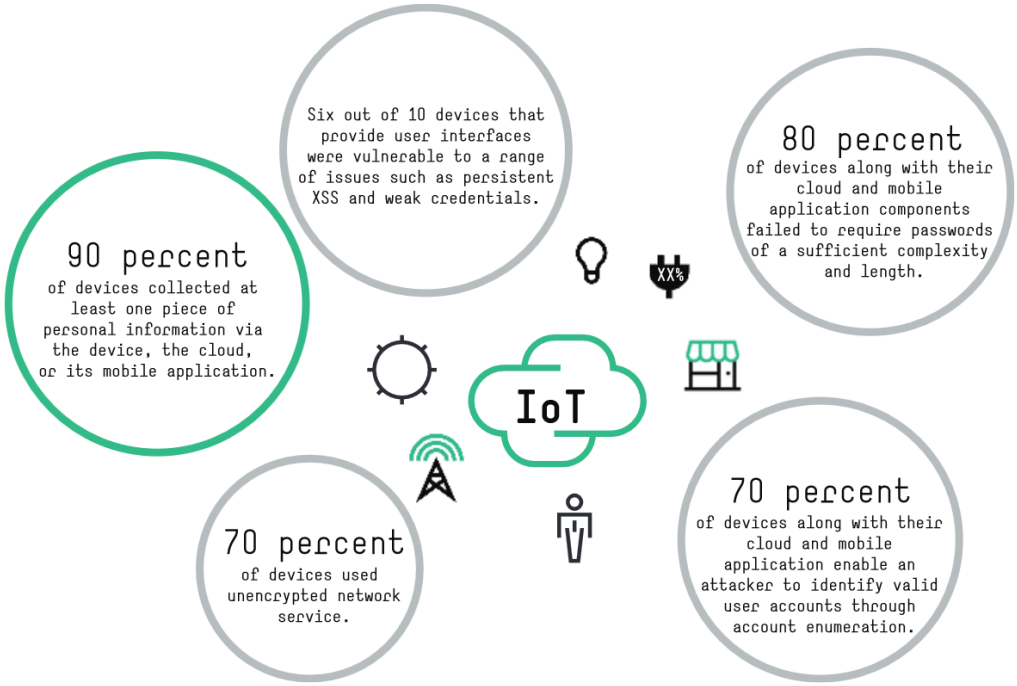

Abbildung 2.5: Internet of Things research study (vgl. Hewlett Packard Enterprise, 2015)

Eine Studie von Hewlett Packard Enterprise, in der Sicherheitsaspekte bei verbreiteten Geräten von Herstellern im Bereich des IoT überprüft wurden, ergab, dass 80% der überprüften Geräte Bedenken hinsichtlich der Privatsphäre aufwirft. Abbildung 2.5 zeigt einige Ergebnisse der Studie. Dabei kam z. B. heraus, dass 70% der Geräte unverschlüsselte Netzwerkdienste verwenden, 80% erlaubten für ihre Cloud- oder App-Anbindung ein schwaches und zu kurzes Passwort und ganze 90% sammelten persönliche Informationen über das Gerät, die Cloud oder die App. Die Studie brachte noch weitere sicherheitsrelevante Schwachpunkte zum Vorschein, die leicht von Angreifern ausgenutzt werden könnten.

3 Aktueller Stand

In diesem Abschnitt werden aktuelle Ergebnisse, Konferenzen und Veröffentlichungen dargestellt.

3.1 Wichtige Konferenzen und Veröffentlichungen

Eine der wichtigsten Konferenzen in diesem Bereich ist der IEEE World Congress on Services[1]. Hier wurde 2015 u. a. das Paper "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things" veröffentlicht, welches schon in Abschnitt 2.2 angesprochen wurde.
Die IEEE Computer Society veranstaltet jährlich fünf Konferenzen im Bereich Service Computing, welche ebenfalls Teile des Internet of Things zum Thema haben:

Cloud Computing Themen zu Modellierung, Entwicklung, Veröffentlichung, Überwachung, Verwaltung und Lieferung von "Everything as a Service" Anwendungen in Verbindung mit Cloud-Umgebungen

Web Services Web-basierte Dienste, mit Web-Services-Modellierung, Entwicklung, Veröffentlichung, Entdeckung, Zusammensetzung, Prüfung, Anpassung und Lieferung, und Web-Services-Technologien sowie Standards

Services Computing Services Innovation Lifecycle umfasst Unternehmensmodellierung, betriebswirtschaftliche Beratung, Lösungserstellung, Orchestrierung der Dienste, Dienstleistungen Optimierung, Service-Management, Marketing-Dienstleistungen, Business Process Integration und Management

[1] http://www.servicescongress.org - letzter Aufruf: 12.03.2016

Mobile Services Entwicklung, Veröffentlichung, Entdeckung, Orchestrierung, Aufruf, Prüfung, Lieferung und Zertifizierung von mobilen Anwendungen und Services

Big Data Quantitative Analyse der Auswirkungen auf die Unternehmen Erkenntnisse aus Big Data Analytics

(vgl. IEEE, 2015)

Auch der Chaos Computer Club[2](CCC) hat sich 2015 stärker auf Sicherheitsaspekte des Internet of Things konzentriert und dabei insbesondere Smart-Homes untersucht. In Zusammenarbeit mit einigen Ministerien entstand daraus zwischen Juni 2015 und Januar 2016 der Leitfaden für Smart-Home-Lösungen[3]. Dieser beinhaltet Empfehlungen für Anbieter und Verbraucher im Smart-Home-Bereich. Der CCC tritt dafür ein, dass kritische Kommunikationsinfrastrukturen starke Sicherheitsstandards erfüllen sollten, daher sind auch in Zukunft Themen im Bereich Internet of Things, Smart-Homes und IT-Sicherheit zu erwarten.

Die IoT Conference (IoTCon) ist ebenfalls ein Treffpunkt für viele Entwickler aus dem IoT-Bereich. Die jährlich in München stattfindende Konferenz bietet Fachvorträgen mit diversen Experten als Speaker auch noch Workshops an. Im Jahr 2015 hat z. B. Jeffrey Katz einen Vortag zum Thema "Privacy and Security in the Internet of Things" gehalten, in dem es darum ging, die Vorteile des IoT zu nutzen, ohne die Privatsphäre und die Sicherheit der Kunden auf's Spiel zu setzen.

Als letzte Quelle für Veröffentlichungen, Paper und Konferenzen soll hier noch auf die Digital Library von ACM eingegangen werden. Hier werden u. a. Paper der SenSys veröffentlicht, der ACM Conference on Embedded Networked Sensor Systems[4].

[2] https://www.ccc.de - letzter Aufruf: 12.03.2016
[3] (vgl. CCC, 2015)
[4] Xu u. a. (2015)

Eine weitere wichtige Konferenz ist hier die ACM Conference on Computer and Communications Security in deren Rahmen der International Workshop on Trustworthy Embedded Devices stattfindet[5].
Des Weiteren bringt ACM Journals heraus, die ebenfalls Themen im Bereich IoT und IT-Sicherheit behandeln. Zum Beispiel das ACM Transactions on the Web Journal oder ACM Transactions on Internet Technology Journal enthalten oft Artikel zu diesen Themen.

Dies sind nur einige ausgewählte Quellen, die in den letzten Monaten einige Ergebnisse und Veröffentlichungen zu den relevanten Fragen zum Internet of Things, Smart-Homes und IT-Sicherheit herausgebracht haben.

[5] Condra (2015)

4 Schluss

In diesem letzten Abschnitt wird noch einmal kurz zusammengefasst, in welche Richtung meine Masterarbeit sich bewegen soll und wie die nächsten Schritte im Grundprojekt aussehen werden.

4.1 Zusammenfassung

Das Internet der Dinge wächst stetig weiter und mit jedem neuen "Ding" steigen auch die Möglichkeiten für Angreifer Informationen oder Zugriffe zu erlangen. Diese Schwachstellen müssen geschlossen werden und die Privatsphäre der Anwender zu schützen und um die Integrität von Daten zu erhalten.
Smart-Homes wachsen mit dem Internet der Dinge, da sie zum Großteil ein System aus verschiedenen "Dingen" darstellen. Ist eins dieser Geräte angreifbar besteht die Möglichkeit darüber das gesamte System anzugreifen. Dies kann unter Umständen einem Angreifer nicht nur eine virtuelle Tür in das Smart-Home öffnen. Die Keyless-Entry Technologie wird auch immer öfter genutzt, sei es im Smart-Home Bereich als auch in Fahrzeugen. Angreifer machen sich die oftmals unverschlüsselt gesendeten Signale zu nutze um sich Zugang zu einem Haus oder einem Fahrzeug zu verschaffen. Im Falle des Fahrzeugs geht es sogar soweit, dass sich das Fahrzeug starten und fahren lässt, ohne dass der Schlüssel entwendet worden sein muss.

4.2 Ausblick

In meiner Masterarbeit möchte ich mich zunächst mit der Keyless-Entry Technologie beschäftigen. Die ersten Schritte werden sein, ein System aufzubauen, welches es

ermöglicht, ein Schloss mit Hilfe eines Smartphones oder ähnlichem zu öffnen, ohne es manuell bedienen zu müssen. Wenn dieses System arbeitet, möchte ich untersuchen, welche Möglichkeiten es gibt, dieses System zu umgehen und das Schloss zu öffnen, ohne in Besitz des Gegenstandes zu sein, der normalerweise dafür benötigt wird.
Die Steuerung des Schlossen wird mit Hilfe von den üblichen Steuergeräten im IoT erfolgen. Die erste Implementierung erfolgt mit einem Raspberry Pi 2 und wird, je nach Bedarf, mit Arduinos ergänzt. Der Aufbau wird im Creative Space der Hochschule für Angewandte Wissenschaften Hamburg erfolgen, wenn das System arbeitet werden Tests im Living Place der Hochschule für Angewandte Wissenschaften Hamburg erfolgen. Ein entsprechendes Schließsystem ist schon vorhanden.
Zum Ende des Grundprojekts soll ein funktionierender Prototyp aufgebaut sein, der sich über ausgewählte Techniken öffnen lässt. Des Weiteren sollen erste mögliche Schwachstellen ausgemacht werden, die ein Angreifer nutzen kann um das System zu umgehen. Außerdem soll Wert darauf gelegt werden, dass das System, wie im IoT üblich, möglichst kompakt und Stromsparend ausgelegt wird und die Leistung trotzdem ausreicht um Mechanismen zu implementieren, die Angriffe verhindern. Im weiteren Verlauf kann die Technik dann auf andere Bereiche, z. B. den Fahrzeugsektor, ausgeweitet werden. Es kann auch getestet werden, in wie weit das Gerät, welches zum öffnen des Schlosses verwendet wird, weitere Verwendung finden kann um beispielsweise Bewegungen zu verfolgen, wie es z. B. mit dem in Abschnitt 2.1 erwähnten MediaCup möglich ist.

Literaturverzeichnis

[Libelium2015] *Libelium Smart World Infographic – Sensors for Smart Cities, Internet of Things and beyond*. http://www.libelium.com/top_50_iot_sensor_applications_ranking/#show_infographic. – Accessed: 2016-03-12

[Ashton 2009] Ashton, Kevin: That Internet of Things Thing. In: *RFID Journal (2009)* (2009). – URL http://www.rfidjournal.com/article/print/4986

[BSI - Bundesamt für Sicherheit in der Informationstechnik 2013] BSI - Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz*. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html. 2013. – Accessed: 2016-03-12

[CCC 2015] CCC: *Leitfaden für Smart-Home-Lösungen*. https://www.ccc.de/en/updates/2016/smarthome. 2015. – Accessed: 2016-03-12

[Condra 2015] Condra, Geremy: A Plea for Incremental Work in IoT Security. In: *Proceedings of the 5th International Workshop on Trustworthy Embedded Devices*. New York, NY, USA : ACM, 2015 (TrustED '15), S. 39–39. – URL http://doi.acm.org/10.1145/2808414.2808424. – ISBN 978-1-4503-3828-8

[Hewlett Packard Enterprise 2015] Hewlett Packard Enterprise: *Internet of Things research study 2015 report*. http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf. 2015. – Accessed: 2016-03-12

[Hossain u. a. 2015] Hossain, M. M. ; Fotouhi, M. ; Hasan, R.: Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In: *Services (SERVICES), 2015 IEEE World Congress on*, June 2015, S. 21–28

[IEEE 2015] IEEE: *IEEE World Congress on Services*. http://www.servicescongress.org. 2015. – Accessed: 2016-03-12

[National Intelligence Council 2008] National Intelligence Council: Disruptive Civil Technologies - Six Technologies with Potential Impacts on US Interests out to 2025 National Intelligence Council (Veranst.), SRI Consulting Business Intelligence, 4 2008. – https://fas.org/irp/nic/disruptive.pdf

[Steinbuch 1966] Steinbuch, Karl: *Die informierte Gesellschaft - Geschichte und Zukunft der Nachrichtentechnik*. 1. Edition. Stuttgart : Stuttgart, dva, 1966, 1966

[Telecooperation Office (TecO) - Institut für Telematik - Universität Karlsruhe 1999] Telecooperation Office (TecO) - Institut für Telematik - Universität Karlsruhe: *MediaCup*. http://mediacup.teco.edu/. 1999. – Accessed: 2016-03-12

[Weiser 1999] Weiser, Mark: The Computer for the 21st Century. In: *SIGMOBILE Mob. Comput. Commun. Rev.* 3 (1999), Juli, Nr. 3, S. 3–11. – URL http://doi.acm.org/10.1145/329124.329126. – ISSN 1559-1662

[Xu u. a. 2015] Xu, Chenren ; Zhang, Pei ; Sigg, Stephan: SenSys'15 Proceedings Workshop Summary Abstract / IoT-App'15: The 2015 International Workshop on Internet of Things Towards Applications. In: *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*. New York, NY, USA : ACM, 2015 (SenSys '15), S. 509–510. – URL http://doi.acm.org/10.1145/2809695.2809697. – ISBN 978-1-4503-3631-4