Sicherheits-Aspekte im Zusammenspiel von Augmented Reality und dem Internet of Things

Hauptseminar Ausarbeitung

Sascha Waltz

Sommersemester 2017

HAW Hamburg

Abstract. In dieser Ausarbeitung wird erklärt, was Augmented Reality ist und wie diese mit Dingen des Internet of Things zusammenarbeiten kann. Des Weiteren wird darauf eingegangen, welche sicherheitstechnischen Aspekte hierbei wichtig sind und beachtet werden müssen. Ziel der Arbeit ist es, die Motivation und die Problemstellung für ein Zusammenspiel der drei Teilbereiche Augmented Reality, Internet of Things und IT-Sicherheit darzustellen.

1 Einleitung

In diesem ersten Abschnitt sollen noch einmal die Probleme und die Motivation erläutert werden, die zu dieser Hauptseminar-Ausarbeitung geführt haben. Außerdem wird ein Überblick über die Kapitel der Arbeit gegeben.

1.1 Motivation

Das Internet der Dinge wächst seit Jahren stetig weiter und es kommen immer neue "Dinge" dazu. Diese werden immer kleiner und komplexer und lassen sich nicht mehr über angeschlossene Displays bedienen. Eine komfortable Möglichkeit bietet hier nun das ebenfalls immer weiter wachsende Feld der Mixed Reality. Speziell der Bereich Augmented Reality ist hierbei von besonderem Interesse. Dieser ermöglicht es, die "Dinge" der Internet of Things über virtuelle Interfaces zu steuern und auf ihre Informationen zuzugreifen. Gleichzeitig werden die Geräte im Internet der Dinge auch immer sensibler. Sollten hier falsche Informationen eingegeben oder Bedienfehler gemacht werden, kann das fatale Folgen haben.

Aktuelle Augmented Reality Brillen ermöglichen die Interaktion über Gesten- oder Sprachsteuerung und somit die Steuerung von Dingen über ein virtuelles Interface. Hier gilt es nun sicherzustellen, dass derjenige, der mit dem Gerät interagieren möchte, auch derjenige ist, der er zu sein vorgibt und vor allem, ob er die nötigen Berechtigungen

vorweisen kann.

Zusätzlich möchte man dem Benutzer aber nicht durch zusätzliche Passworteingaben oder andere Interaktionen die eigentliche Benutzung erschweren. Also sollte die Authentifizierung und die Autorisierung möglichst ohne Zutun des Benutzers erfolgen, ähnlich wie bei aktuellen Keyless-Entry-Systemen, bei denen es ausreicht einen Schlüssel mit Sender oder sogar nur einen RFID-Chip bei sich zu tragen.

Das Zusammenspiel von Authentifizierung/Autorisierung, Interaktion und Kommunikation soll somit die Motivation für diese Ausarbeitung sein.

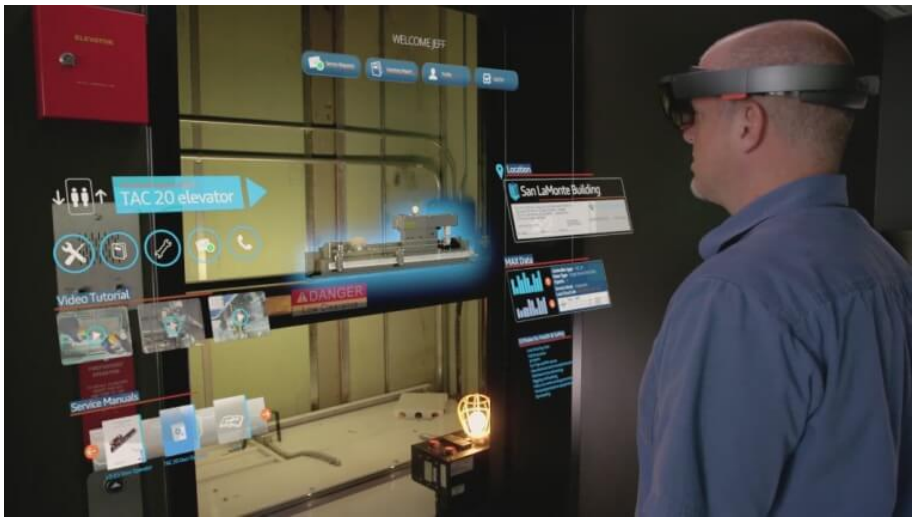

Fig. 1. Vision zur Wartung von Fahrstühlen per AR-Interface von thyssenkrupp Elevator [3]

1.2 Aufbau der Arbeit

Das folgende Kapitel wird sich zunächst mit Augmented Reality beschäftigen und aufzeigen, was AR überhaupt bedeutet, welche Möglichkeiten es gibt und wo die Grenzen sind.

Das darauf folgende Kapitel gibt noch einmal einen kurzen Überblick über das Internet der Dinge, dessen Wachstum und den Umfang.

Kapitel 4 befasst sich dann mit den Aspekten der IT-Sicherheit und deren Realisierung auf “Dingen“ des IoT.

Wenn die drei involvierten Bereiche erklärt und veranschaulicht wurden, wird das Zusammenspiel anhand eines Szenarios und die eigentliche Problemstellung erklärt.

Zum Abschluss gibt es dann einen Ausblick auf die weiterführende Planung und eine Zusammenfassung dieser Ausarbeitung.

2 Augmented Reality

Die erweiterte Realität, oder Augmented Reality (AR), beschreibt die computergestützte Erweiterung der Realität durch zusätzliche Informationen.

> Augmentierte Realität ist eine (unmittelbare, interaktive und echtzeitfähige) Erweiterung der Wahrnehmung der realen Umgebung um virtuelle Inhalte (für beliebige Sinne), welche sich in ihrer Ausprägung und Anmutung soweit wie möglich an der Realität orientieren, so dass im Extremfall (so das gewollt ist) eine Unterscheidung zwischen realen und virtuellen (Sinnes-) Eindrücken nicht mehr möglich ist. [6, S. 246]

Hierbei werden die Informationen, Bilder oder sogar Animationen für den User über die reale Welt eingeblendet. Durch den enormen technischen Fortschritt in diesem Bereich und in der Virtual Reality in den letzten Jahren, lassen sich heutzutage noch viele weitere Dinge per Augmented Reality einblenden, so z.B. dreidimensionale oder bewegliche Objekte, Videos oder auch Videoanrufe.
Auch wenn AR in den Medien erst seit kurzen immer präsenter wird, ist es schon seit anfang der 90er Jahre in der Entwicklung. Bereits im Paper *Augmented Reality: A class of displays on the reality-virtuality continuum* [8] aus dem Jahr 1994 beschreiben die Autoren ““See-through“ AR displays“ und “Monitor based AR displays“. Ebenso wird in diesem Paper die Augmented Reality so zur Mixed Reality abgegrenzt, als dass in der AR der Anteil der Realität deutlich überwiegt und der Nutzer primär mit seiner Realität interagiert.
Um sich vorzustellen, welche Unterschiede zwischen Augmented, Mixed und Virtual Reality bestehen, lassen sich folgende Abgrenzungen festlegen:

Augmented Reality ist eine reale Umgebung mit virtuellen Objekten
Mixed Reality ist eine virtuelle Umgebung mit realen Objekten
Virtual Reality ist eine virtuelle Umgebung mit virtuellen Objekten

Fig. 2. Zusammensetzung einer Augmented Reality [6]

Hierbei handelt es sich in der Regel nicht immer nur um Objekte, auch Interfaces können zur Interaktion in die reale oder virtuelle Welt projiziert werden.
In vielen Fällen lassen sich die AR-Interfaces gut mit Dingen aus dem Internet of Things verbinden, die entsprechende Daten zur Anzeige im AR-Interface liefern. Dies können

Informationen zu Gebäuden oder zum Wetter sein, ebenso wie zu anderen Personen, Fahrzeugen oder Dingen.

Am weitesten verbreitet sind Anwendungen für Augmented Reality für Smartphones oder Tablets, die mit Hilfe der integrierten Kamera das Bild der Umgebung aufzeichnen und auf dem Display die virtuellen Objekte über die gefilmte reale Umgebung legen.

Zur Zeit im Kommen sind AR-Brillen, welche einen durchsichtigen Bildschirm vor den Augen des Anwenders positionieren, in den die virtuellen Objekte eingeblendet werden, während man die Umgebung durch den Bildschirm immer noch sehen kann.

2.1 Interaktion in Augmented Reality

Die Möglichkeiten zur Interaktion in AR und VR Umgebungen werden immer vielfältiger und komplexer, so gibt es die Möglichkeit, mit Hilfe eines Eingabegerätes wie z.B. einer Fernbedienung oder eines Smartphones zu interagieren, als auch die Möglichkeit mit Bewegungen, Gesten oder Geräuschen die Eingabe zu steuern.

Die aktuellen AR-Brillen, wie z.B. Microsofts Hololens, werden ausschließlich über

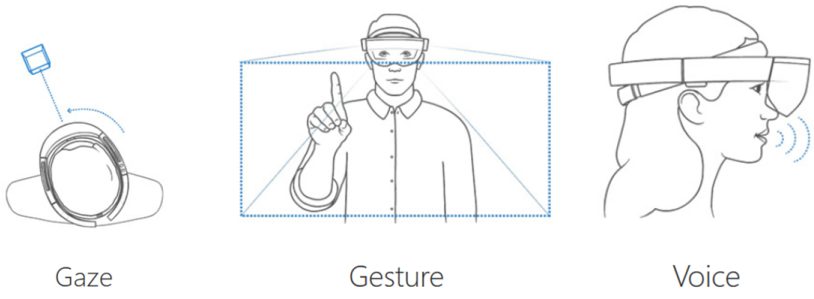

Fig. 3. Interaktionsmöglichkeiten mit Augmented Reality [7]

Gesten, die der Anwender im Sichtfeld der Brille durchführt, und die Blickrichtung, oder komplett per Spracheingabe bedient. So kann der Anwender mit den Objekten interagieren oder sie verändern. Figure 3 zeigt die Interaktionen die Hauptsächlich in diesem Kontext genutzt werden.

Diese Interaktionsmöglichkeit haben Firmen entdeckt um mit Hilfe von in der Augmented Reality verborgenen Interfaces ihre Maschinen und Geräte zu steuern. So hat unter Anderem die Firma *thyssenkrupp Elevator* ein Video veröffentlicht, wie sie sich die Wartung ihrer Fahrstühle in Zukunft per AR vorstellt [1].

Egal auf welche Weise die Interaktion vonstatten geht, es wird immer eine Anwendung in Form einer App auf der entsprechenden AR-Brille benötigt. Diese Apps projizieren

[1] https://www.youtube.com/watch?v=8OWhGiyR4Ns - Abgerufen: 04.03.2017

die die Objekte, Interfaces oder Texte in die reale Umgebung und steuern die Interaktion des Users über ein Eingabegerät oder die entsprechenden Gesten.

3 Internet of Things

In diesem Kapitel wird dargestellt, was das Internet der Dinge (IoT) umfasst und leistet und wie seine Entwicklung vonstatten geht.

3.1 Entwicklung und Umfang

Das Internet der Dinge wächst stetig weiter und umfasst immer mehr Geräte die durch ihre Vernetzung in der virtuellen Welt präsent gemacht werden. Wie in Figure 4 zu

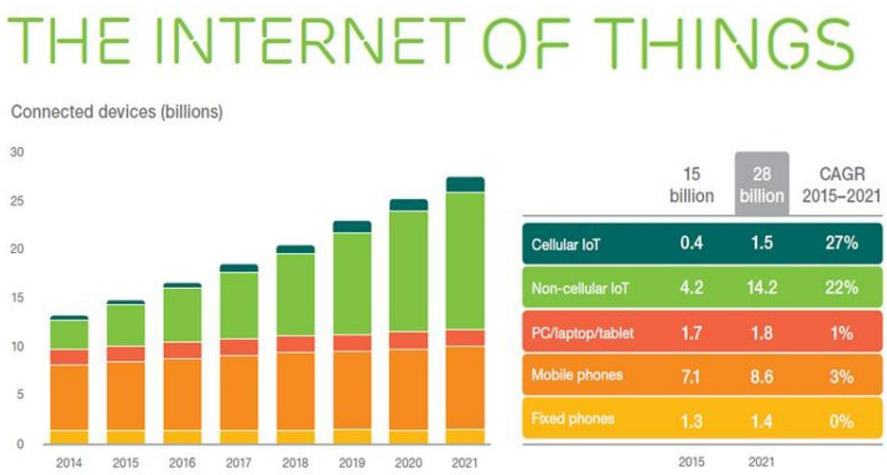

Fig. 4. Mit dem Internet verbundene Geräte [2]

sehen, wächst das IoT bis 2020 so weit, dass die Anzahl der Geräte den Großteil der im Internet auftauchenden Geräte ausmacht.

All diese Geräte sammeln Daten und stellen sie zur Verfügung oder lassen sich verwenden um Ereignisse auszulösen oder sie reagieren einfach nur auf Ihre Umwelt. In der Regel handelt es sich bei solchen “Dingen“ um kleine, unsichtbare Geräte, die ihre Aufgabe verrichten, ohne dass jemand sie bewusst wahrnimmt und dennoch werden sie täglich von diversen Menschen genutzt. Das *National Intelligence Council* hat auf einer Konferenz im Jahr 2008 eine Roadmap für das IoT veröffentlicht, nach der wir uns zur Zeit im Abschnitt “locating people and everyday objects“ befinden, also die Bestimmung und Wahrnehmung von Positionen von Personen oder Objekten. Dazu kommen natürlich noch die diversen Daten die durch Sensoren gesammelt und aufgearbeitet werden können, damit Objekte sich ihrer Umgebung bewusst sind und automatisch auf

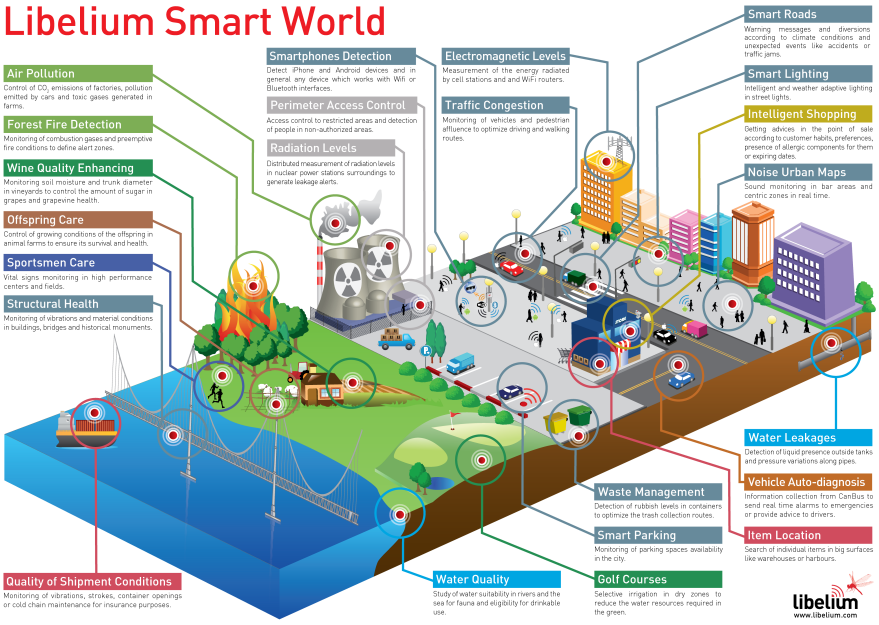

Fig. 5. Libelium Smart World [1]

sie reagieren können. In Figure 5 sieht man eine Vision der Firma Libelium, vorgestellt auf dem “Meeting of the Minds – Smart Cities 2.0: What Works Today“ im November 2015. Diese Grafik zeigt, welche Dinge bis zum Jahr 2020 im Internet of Things vernetzt sein könnten. Viele dieser Dinge sind nur zum Sammeln von Daten da, einige reagieren auf Ihre Umwelt und lösen so entsprechende Ereignisse aus. Aber es gibt auch “Dinge“, mit denen Menschen bewusst interagieren können, wie z.B. Informationstafeln.

Oft fallen in Verbindung mit dem Internet der Dinge auch Begriffe wie Ubiquitous Computing, Pervasive Computing, Ambient Intelligence oder Silent Commerce. Alles Begriffe, die aussagen, dass sich hier Computer in die Umgebung eingliedern und mit ihr verschmelzen. Um dennoch kommunizieren zu können, müssen sich die einzelnen Geräte kabellosen Technologien bedienen, in der Regel kommen Techniken zum Einsatz, die wenig Energie verbrauchen und somit nur über kurze Distanzen effektiv arbeiten, wie z.B. Bluetooth, RFID oder LowPAN.

Die Sicherheitsaspekte, die in section 4 behandelt werden, werden bei den Geräten im Internet der Dinge oft vernachlässigt und ermöglichen es so z.B. die Geräte für Angriffe zu missbrauchen, wie Ende 2016 mit dem so genannten Mirai-Botnetz geschehen. Dieser Angriff war der bis dahin größte DDoS-Angriff mit circa 1,2 TBps [10].

4 IT-Sicherheit

Wie schon im Grundseminar [9] erwähnt, ist IT-Sicherheit auch im Internet der Dinge unverzichtbar. Nach wie vor müssen die folgenden Punkte auch im Internet der Dinge gewährleistet sein:

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.

(vgl. [9]) Im IoT sind die Möglichkeiten Sicherheitsaspekte umzusetzen recht begrenzt, da die "Dinge" eine recht begrenzte Kapazität haben, das Leistung, Energieverbrauch und Speicher angeht. Dennoch gibt es verschiedene Möglichkeiten um im IoT Sicherheit zu realisieren (vgl. [4]):

security architecture Die Sicherheitsarchitektur beschreibt, wie Sicherheitsaspekte zwischen den Dingen umgesetzt werden und wie Dinge in Ihrem Lebenszyklus in die Architektur eingebunden, behandelt und am Ende wieder ausgegliedert werden.

security model of a node Das Sicherheitsmodel eines Dinges beschreibt, wie Sicherheitsparameter, Prozesse und Anwendungen innerhalb eines Dinges geregelt werden.

Security bootstrapping Das Security bootstraping regelt, wie ein Ding zu einem Zeitpunkt sicher in das Internet der Dinge eingegliedert wird. Hierzu gehört ebenfalls die Authentifizierung und Autorisierung eines Gerätes und die Übertragung der Sicherheitsparameter für zukünftige vertrauenswürdige Operationen.

Network security Netzwerksicherheit umfasst sowohl das sichere Routing als auch die Festlegung von Mechanismen um sichere Operationen innerhalb des Netzwerkes sicherzustellen.

Application security Anwendungssicherheit bedeutet hier, dass nur vertrauenswürdige Instanzen von Anwendungen auf dem Gerät laufen mit anderen Geräten im Netzwerk oder im IoT kommunizieren darf. Außerdem muss hier sichergestellt sein, dass nicht vertrauenswürdige Instanzen sich nicht in die Kommunikation einschalten können.

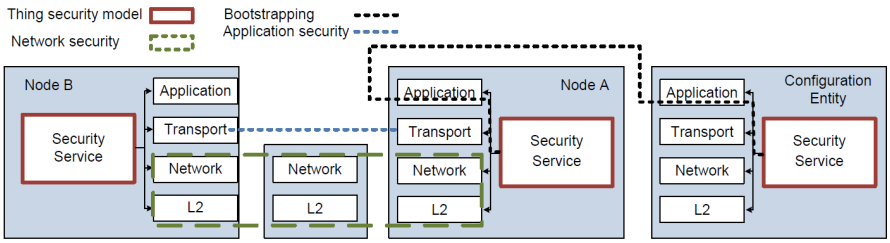

Fig. 6. IT-Sicherheit im Internet der Dinge [4]

Es gibt verschiedene Möglichkeiten im IoT die Authentizität einer Komponente sicherzustellen. An dieser Stelle sollen nur 2 der gängigsten erwähnt werden:

Mutual Authentication In einer Netzwerkumgebung können sich Geräte untereinander mit Zertifikaten authentifizieren und somit eine vertrauenswürdige Kommunikation gewährleisten. Dies wird durch eine hybride Verschlüsselung und durch Zertifikate realisiert.

Trusted Network Connect Neben der Authentifizierung unter Geräten ist es ebenfalls möglich, alle Zugriffe innerhalb eines Netzwerks zu analysieren und somit die Sicherheit zu erhöhen. Dies ist ein offener Standard, der von der Trusted Network Group entwickelt wurde.

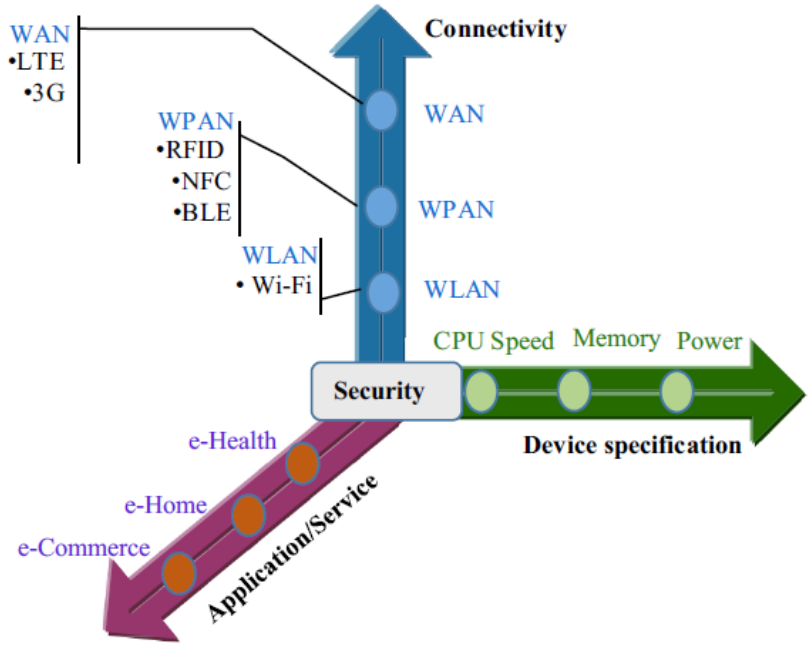

Fig. 7. Security Landscape IoT(vgl. [5])

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 Figure 7 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. (vgl. [9])

5 Zusammenspiel und Problemstellung

In diesem Abschnitt soll nun verdeutlicht werden, wie diese 3 Bereiche, Augmented Reality, Internet der Dinge und IT-Sicherheit zusammen hängen und welche Problemstellungen es zu lösen gilt.

5.1 Szenario: Fahrstuhlwartung

Wie schon in section 2 erwähnt wurde, hat die Firma *thyssenkrupp Elevator* ein Konzept zur Wartung ihrer Fahrstühle entwickelt, bei dem es einem Techniker ermöglicht

[2] [5]

wird, auf die Funktionen des Fahrstuhls mit Hilfe von Microsofts Hololens AR-Brille zuzugreifen, mit diesem zu Interagieren und so schnell und unkompliziert eine Wartung durchzuführen. Da die Systeme eines Fahrstuhls aber sehr kritische Systeme sein können und nur von Fachpersonal gewartet werden dürfen, muss an dieser Stelle sichergestellt sein, dass die Person, die gerade versucht über das AR-Interface auf die Fahrstuhl-Systeme zuzugreifen, hierzu auch berechtigt ist.

Man könnte nun zum einen überprüfen, ob die Hololens-Brille ein entsprechendes Zertifikat besitzt oder die entsprechende Anwendung um das Interface zu sehen. Allerdings kann so eine Brille auch verloren gehen oder gestohlen werden. Ebenso kann die Software kopiert oder gestohlen werden. Somit ist der Besitz der entsprechenden Brille kein eindeutiger Indikator dafür, dass die Person, die diese Brille nutzt auch die entsprechende Berechtigung besitzt.

5.2 Zusammenspiel

Wie das obige Szenario schon verdeutlicht, lassen sich Dinge im IoT, wie z.B. der Fahrstuhl, über ein AR-Interface steuern. Der Vorteil hierbei ist, dass die "Dinge" möglichst klein gehalten werden können, da keine Anzeigefläche benötigt wird. Die Kommunikation der Dinge untereinander muss hierbei wie in section 4 beschrieben abgesichert sein, aber auch der Zugriff auf das AR-Interface muss gesichert werden, um nur berechtigten Personen Zugriff zu gewähren. Hier kommt wieder die Authentifizierung und Autorisierung zum tragen, bei denen festgestellt werden muss, wer Zugriff erlagen möchte und ob diese Person dazu berechtigt ist.

5.3 Problemstellung

Das Zusammenspiel der 3 Bereiche ist zunächst das erste Problem. Hier stellen sich Fragen wie "Wie soll die Kommunikation realisiert werden?", "Wie wird die Kommunikation abgesichert?" oder "Welche Parameter der Umgebung müssen berücksichtigt werden?".

Das eigentliche Problem liegt hier aber im IT-Sicherheitsbereich. Hier muss überlegt werden, welche Möglichkeiten es gibt, um sicherzustellen, dass der Benutzer der Brille auch derjenige ist, der er behauptet zu sein und das dieser die Berechtigung zur Nutzung der Funktionen des Gerätes besitzt. Außerdem sollte der Benutzer nicht zusätzlich durch diese Sicherheitsmaßnahmen beeinträchtigt werden, also kein extra Passwort eingeben oder z.B. eine Schlüsselkarte benutzen müssen. Des Weiteren müssen die Sicherheitsmaßnahmen auf einem Gerät des IoT realisierbar sein und dürfen hier nicht übermäßig lange Zeit für die Überprüfung in Anspruch nehmen.

6 Ausblick und Zusammenfassung

Zum Abschluss der Ausarbeitung soll hier noch ein Ausblick auf die weiterführende Planung und eine Zusammenfassung der Arbeit gegeben werden.

6.1 Ausblick

Die nächsten Schritte werden im Hauptprojekt durchgeführt. Hier soll eine Versuchsumgebung aus einigen Geräten für das Internet der Dinge aufgebaut werden. Für diese werden dann einige einfache Interfaces aufgebaut, die auf der Hololens von Microsoft laufen werden. Sobald die Bedienung in dieser Versuchsumgebung funktioniert, werden die Sicherheitsaspekte umgesetzt. Zunächst mit Hilfe von Zertifikaten und dann in einer Keyless-Variante.

Es soll dabei hauptsächlich darum gehen, dass die Authentifizierung von Benutzern zuverlässig, sicher und schnell funktioniert, die Gestaltung von AR-Interfaces soll dabei nicht im Vordergrund stehen und kann in Zukunft in einer anderen Arbeit behandelt werden.

Ziel soll die Interaktion eines Authentifizierten Benutzers mittels AR-Interface mit einem Ding im Internet of Things sein.

6.2 Zusammenfassung

In dieser Ausarbeitung wurde die Motivation dargelegt, die zu der in section 5 genannten Problemstellung geführt hat. Die Lösung dieser Problemstellung soll im Hauptprojekt umgesetzt und letztendlich in der Masterthesis ausgearbeitet werden. Außerdem wurde ein Überblick über das Zusammenspiel zwischen Dingen des Internet of Things, Augmented Reality Interfaces und IT-Sicherheit gegeben. Um dies zu tun wurde zunächst ein Einblick in die drei Teilbereiche geschildert und darauf eingegangen, welche Aspekte der einzelnen Bereiche im Zusammenspiel wichtig sind.

References

1. 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
2. Columbus, L.: Roundup of internet of things forecasts and market estimates, 2016 (2016), https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#2b2644f6292d
3. Dressler, N.J.: Thyssenkrupp setzt hololens für aufzugsentwicklung und -service ein (2016), http://winfuture.de/news,94026.html
4. Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S., Wehrle, K.: Security challenges in the ip-based internet of things. Wireless Personal Communications 61(3), 527–542 (2011), http://dx.doi.org/10.1007/s11277-011-0385-5
5. 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. pp. 21–28 (June 2015)
6. van Looy, A.: Der digitale Raum: Augmented und Virtual Reality, pp. 51–62. Springer Fachmedien Wiesbaden, Wiesbaden (2017), http://dx.doi.org/10.1007/978-3-658-16509-3_3
7. Microsoft: Why hololens (2016), https://www.microsoft.com/microsoft-hololens/de-de/why-hololens
8. Milgram, P., Takemura, H., Utsumi, A., Kishino, F.: Augmented reality: a class of displays on the reality-virtuality continuum (1995), http://dx.doi.org/10.1117/12.197321

9. Waltz, S.: It-sicherheit im umfeld des internet of things. Tech. rep., Hochschule für Angewandte Wissenschaften Hamburg, http://users.informatik.haw-hamburg.de/ ubicomp/projekte/master2015-gsem/waltz/bericht.pdf (2016)
10. Woolf, N.: Ddos attack that disrupted internet was largest of its kind in history, experts say (2016), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet