Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorthesis

Vor- und Zuname:
Wiliam Mahyar

[redacted]

Titel:

„Gestaltung von Cybersecurity im vernetzten Automobil“

Abgabedatum: 11.09.2020

Betreuender Professor: Herr Prof. Dr. Roehrs
Zweiter Prüfer: Herr Prof. Dr. Lenschow

Fakultät: Wirtschaft und Soziales
Department: Wirtschaft
Studiengang: Logistik / technische Betriebswirtschaftslehre

Zusammenfassung

Der Umbruch des Digitalen Wandels hat auch die Automobilindustrie erreicht und sorgt für eine zunehmende Vernetzung verschiedener Fahrzeugsysteme. Dieses heranwachsende Netz bringt einige, neue Risiken bezüglich der Sicherheit mit sich. Somit ist es das Ziel der Forschung, abgestimmt auf den Nutzer vernetzter Fahrzeuge, die gewährleistete Cybersecurity zu bestimmen.

Aus diesem Grund sind zunächst die drei Begriffe Funktionssicherheit, Cybersecurity und Datenschutz relevant. Es wird analysiert, welche Maßnahmen und Standards in der Automobilindustrie bereits existieren und was im Engineering bezüglich verschiedener Verschlüsselungen zu beachten gilt. Basierend auf diesen Grundlagen wird folgend die Theorie auf ein Szenario aus der Praxis übertragen. Mit diesen Erkenntnissen werden zuletzt in Form einer SWOT-Analyse die Stärken und Schwächen sowie die Chancen und Risiken der Cybersecurity in der Automobilwelt gegenübergestellt. Die Basis der Bachelorarbeit ist das Beispielszeanrio des Hackerangriffes auf den Jeep Cherokee, durchgeführt von Charlie Miller und Chris Valasek im Jahr 2014.

Zentrale Ergebnisse der Arbeit sind, dass es absolute Cybersecurity bei vernetzten Fahrzeugen nicht geben wird und dennoch, zur Steigerung der Sicherheit, enorme Entwicklungspotenziale besonders in den Bereichen der Ausweitung weiterer Standards, der neuen Art von Over-the-Air-Updates und der allgemeinen Fokussierung auf das Thema Sicherheit in der Gesellschaft liegen.

Inhaltsverzeichnis

Abkürzungsverzeichnis

A

ABS *Antiblockiersystem*
AES *Advanced Encryption Standard*
ASIL *Automotive Safety Integrity Level*

C

C2C *Car-to-Car*
C2E *Car-to-Enterprise*
C2H *Car-to-Home*
C2I *Car-to-Infrastructure*
CAN *Controller Area Network*

D

DoS *Denial of Service*

E

eCall-System *Emergency call System*
ESC *Electronic Stability Control*

F

FuSi-Standard *Funktionale Sicherheit-Standard*

G

GPS *Global Positioning System*

H

HEAVENS *HEAling Vulnerabilities to ENhance Software Security and Safety*

I

ISO *Internationale Standardisierungs Organisation*
IT *Informationstechnik*

K

KI *Künstliche Intelligenz*

L

LIN *Local Interconnect Network*

M

MOST *Media Oriented Systems Transport*

N

NIST *National Institute of Standard and Technology*

O

OBD *On Board Diagnose*
OEM *Original Equipment Manufacturer*
OTA *Over-the-Air*

P

PQC *Post-Quantum-Cryptography*

R

RFID *Radio Frequency Identification*
RSA-Verfahren *Rivest-Shamir-Adleman-Verfahren*

S

SPICE *Software Process Improvement and Capability Evaluation*
STRIDE *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*

T

TARA *Threat Analysis and Risk Assessment*

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

1.1 Problemstellung und Zielsetzung

Ein kurzer virtueller Abstecher zur Familie, ein Film zur Entspannung oder das morgendliche Frühstück auf dem Weg zum Geschäftskunden – solche Bilder sind bereits in den Köpfen der Menschen verankert, wenn sie an zukünftige Autofahrten denken. Während die Aufmerksamkeit dem Biss in das Croissant gewidmet ist, kommuniziert das Fahrzeug mit der Umwelt, um brenzliche Gefahrensituationen zu vermeiden. Der Blick auf das Handy und das Überprüfen der Nachrichten stellt plötzlich keine Gefahrensituation mehr dar, sondern viel mehr die alltägliche Routine im Auto. Durch die Vernetzung verschiedenster Fahrzeugsysteme und dem Einzug des Internet of Things (zu Deutsch: Internet der Dinge) in das Automobil sind diese Beispielszenarien schon heute nahe Realität.[1]

Getrieben von der Version Zero, einer emissions- und unfallfreien Straße, wird die digitale Revolution des Autos hin zur Konnektivität intensiv gepusht. Den Fahrzeugen dank der KI (Künstliche Intelligenz) das menschliche Fühlen und Sehen beibringen, ist die Zukunftsvision vieler Automobilhersteller.[2]

Und während in den 1886 Jahren die Erfindung des Automobils als Ablöse des Fortbewegungsmittels von Pferd und Kutsche zu der bahnbrechendsten Erfindung zählte, reizt Elon Musk den Vergleich auf die heutige Situation noch weiter aus, indem er sagt: „In 20 Jahren wird sich der Besitz eines Autos, das nicht autonom fährt, anfühlen wie heute der Besitz eines Pferdes.“[3]

Doch wo die Sonne scheint, da ist auch Schatten. Durch stärkere Vernetzung, zusätzliche Schnittstellen und Funktionalitäten wird auch die Attraktivität eines Angriffes auf Fahrzeuge und die angebundene Infrastruktur durch Hacker mit unterschiedlicher Motivation erhöht.

---

[1] Vgl. Johanning, V./Mildner, R. 2015, S. 1.

[2] Vgl. Schleicher, M. 2020, S. 1 ff.

[3] Vgl. Elon Musk 2020c (online, URL siehe Literaturverzeichnis).

Auch durch den zunehmenden Grad an Automatisierung ist es notwendig, entsprechende Fahrzeugfunktionen durch Security-Maßnahmen gegen manipulierte Eingriffe zu schützen. So zeigten Charlie Miller und Chris Valasek bereits im Jahr 2015 große Sicherheitslücken auf: Das Horrorszenario, die Kontrolle über das eigene Auto zu verlieren, wird erstmals greifbar. Sie hackten ein fahrendes Auto, welches 15 Kilometer von dem Computer entfernt war und konnten Bremsen, Radio, Gas und Scheibenwischer übernehmen. Hierbei gelang es ihnen verschiedene Schwachstellen gleichzeitig auszunutzen – hinreichend vom Konnektivitätselement bis zur mangelnden Isolation diverser fahrzeuginterner Systeme.[4]

Eine sichere Entwicklung der Fahrzeugsysteme hängt von dem Zusammenspiel neuer Verbindungen und dessen geprüften Sicherheitsarchitektur ab. Hierbei gibt es verschiedene Möglichkeiten bei der Implementierung von vernetzten Systemen zu beachten, wie der OEM (Original Equipment Manufacturer zu Deutsch: Erstausrüster) dem potentiellen Angreifer oder der funktionalen Gefahr eine möglichst kleine Angriffsfläche bieten und den Insassen schützen kann.

Somit gilt es als Ziel dieser Arbeit, die folgende Frage zu beantworten:

„Inwiefern kann den Nutzern von vernetzten Fahrzeugen eine absolute Cybersecurity gewährleistet werden?“

Demnach werden in der vorliegenden Arbeit verschiedene Szenarioanalysen aufgezeigt und die Begriffe der Cybersecurity und des Cybercrimes im vernetzten Automobil gegeneinander aufgespielt, um das Angriffs- bzw. Schutzpotenzial des jeweiligen Pols zu symbolisieren.

[4] Vgl. Cybersecurity Roadmap 2020d (online, URL siehe Literaturverzeichnis).

1.2 Aufbau der Arbeit

Um einen inhaltlichen Überblick über das Themenfeld des vernetzten Automobils zu schaffen, steigt die Thesis mit grundlegenden Definitionen des Connected Cars ein. Auf Basis dieser Erklärung wird die Architektur der relevanten Systeme, sowohl intern als auch extern, veranschaulicht. Diese Verzahnungen der modernen IT (Informationstechnik) werden im 4. Kapitel auf Sicherheit geprüft.

Hierfür werden zunächst die Begriffe funktionale Sicherheit, Cybersecurity und Datenschutz theoretisiert und im späteren Verlauf auf die Praxis übertragen und anhand von Beispielen realisiert. Die anschließende Diskussion dient der Gegenüberstellung bestehender Stärken und Schwächen, sowie Chancen und Risiken, bezüglich der gegebenen bzw. fehlenden Sicherheit im vernetzten Automobil. Im abschließenden Fazit wird der Inhalt der Arbeit kurz zusammengefasst und ein Ausblick in die zukünftige Entwicklung der Automobilindustrie gegeben.

2. Car IT im vernetzten Automobil

2.1 Definition Connected Cars

Der Begriff des Connected Cars (zu Deutsch: vernetztes Auto) wurde im Zuge der Digitalisierung des Autos geschaffen. Um auf das Connected Car einzugehen, müssen zunächst einmal die Grundlagen zu Fahrzeugsystemen definiert werden. Ein Fahrzeugsystem besteht aus den Wörtern „Fahrzeug“ und „System“, wobei ein System ein Gefüge von einzelnen Bestandteilen ist, die gemeinsam eine bestimmte Funktion verwirklichen. Folglich ist ein Fahrzeugsystem ein Gefüge aus einzelnen Bauteilen, die eine Funktion ausüben.[5] Dabei besteht solch ein Fahrzeugsystem aus Sensor, Aktor und Steuergerät. Um ein Beispiel für ein Fahrzeugsystem und seine Funktionsweise zu nennen, wird ein Airbagsystem näher erläutert.

[5] Vgl. Holland, H. 2019, S. 51 ff. (online, URL siehe Literaturverzeichnis).

Hierbei wird durch die Sensoren des Airbagsystems eine Verformung der Karosserie erkannt, diese Information wird dann anschließend an das Steuergerät weitergeleitet und die Aktoren führen den Befehl des Aufblasens der Airbags aus.[6]

Der Unterschied zwischen einem Fahrzeugsystem und einem vernetzten Fahrzeugsystem liegt in der Kommunikationsfähigkeit des Steuergeräts. Die Konnektivität beschreibt hierbei ein System, welches aus einzelnen Elementen in einem Ursache-Wirkungsverhältnis besteht und besondere Systemeigenschaften miteinander verknüpft. Die Betrachtung dieser Erklärung unter der Prämisse des Automobils ergibt einen ersten Definitionsansatz des Connected Car.[7]

Hierbei gilt es das Internet of Things als Drahtzieher zu betrachten, der die einzelnen Systeme miteinander kommunizieren lässt und das Automobil somit online stellt. Sobald das Auto als online einzustufen ist, welches beispielsweise aus der Verbindung eines Smartphones mit dem Auto oder auch mit der SIM-Karte im Auto besteht, wird von einem Connected Car gesprochen. In Fachkreisen wird auch von Car IT gesprochen, da die neuen Funktionen des Fahrzeugs gänzlich nicht mehr aus der Elektronik bestehen, sondern vielmehr auf der IT basieren. Eine allgemeingültige Definition von Car IT existiert nicht, da das Themengebiet momentan noch zu unerforscht und dynamisch ist.[8]

Weiterhin ist zu sagen, dass diese Bachelorarbeit sich nicht mit dem Themenfeld des autonomen Fahrens beschäftigt, wobei einige Kommunikationsmodelle vorgestellt werden, welche eine Vorstufe des autonomen Fahrens darstellen. Der Fokus dieser Arbeit liegt somit auf der allgemeinen Vernetzung des Automobils und den dafür notwendigen Systemen.

---

[6] Vgl. Borgeest, K. 2008, S. 3 ff.

[7] Vgl. Graf, F., S. 2 ff.

[8] Vgl. Johanning, V./Mildner, R. 2015, S. 1 ff.

2.2 Funktionsweise vernetzter Fahrzeugsysteme

2.2.1 Interne IT-Architektur im Automobil

Ein Fahrzeug-Bordnetz besteht aus ca. 80 verschiedenen Steuergeräten, die im Gesamtkonstrukt das Auto sowohl mit der Außenwelt als auch untereinander, kommunikationsfähig machen. Ein Steuergerät, wie weiter oben erwähnt, verarbeitet Sensorinformationen des Fahrzeugs und besteht grundsätzlich aus Hard- und Software. Als Fundament für die Vernetzung wird die Mobilfunkverbindung mit Backendsystemen der Hersteller gesehen, die das Auto schlussendlich mit dem Internet verbinden.[9]

Fahrzeuge sind heutzutage sehr breit aufgestellt, was ihre Ausstattungsweisen der intern befindlichen Fahrzeugbordnetzarchitektur betrifft. Zum einen findet sich das Motorsteuergerät, Getriebesteuergerät sowie etwaige Sensoren und die Wegfahrsperren im Antriebsbereich, zum anderen befinden sich Bremssteuergeräte, wie z.B. ESC (Electronic Stability Control) und ABS-Steuerung (Antiblockiersystem), Servolenkungssteuergeräte, das Airbagsteuergerät, einige Sensorsteuergeräte, die beispielsweise für die Reifendrucksensoren benötigt werden und Steuergeräte, die mit anderen Steuergeräten kommunizieren, wie z.B. Spurhalteassistenten, im Fahrzeug und werden dem Bereich des Fahrgestells bzw. der Sicherheit zugeordnet. Im Bereich des Fahrgastraumes befinden sich Ausstattungsmerkmale wie das Kombiinstrument, welches das Tachometer oder auch den Kilometerzähler anzeigt. Zum Kombiinstrument zählen weiterhin noch: Drehzahlmesser, Tankanzeige, Kühlmitteltemperaturanzeige und Kontrollleuchten für sämtliche Fehlermeldungen im Fahrzeug. Steuergeräte zur Sitzeinstellung, Türöffnung und die Klimaanlage zählen ebenso zum Fahrgastraum.[10]

Die Head Unit befindet sich im Armaturenbrett des Fahrzeugs und bildet eine weitere Schnittstelle. Das Infotainment, welches aus den Wörtern Information und Entertainment (zu Deutsch: Unterhaltung) besteht, ist zuständig für das Navigationssystem, Audio, Video und Telefon.

---

[9] Vgl. Krauß, C./Waidner, M. 2015, S. 383.

[10] Vgl. ebenda, S. 383 f.

Diese Ausstattungsmerkmale kommunizieren hauptsächlich über die Head Unit. Jene kann durch eine Kopplung mit beispielsweise einem Smartphone eine Internetverbindung aufbauen. Die Kopplung des Smartphones findet grundsätzlich per USB oder Bluetooth statt. Per Kopplungsanfrage wird die Erlaubnis eingeholt, personenspezifische Smartphone-Daten mit dem Fahrzeug zu synchronisieren, welche beispielsweise als Anruflisten über den Infotainment Bildschirm ausgestrahlt werden.[11]

Nun stellt sich die Frage, wie die einzelnen Steuergeräte im Fahrzeug miteinander kommunizieren, um leistungsfähig zu werden. Die Steuergeräte kommunizieren über Bus-Systeme wie z.B. CAN (Controller Area Network), LIN (Local Interconnect Network), MOST (Media Oriented Systems Transport), Flexray oder auch Ethernet. Aber nicht nur die Kommunikation per Kabel ist möglich, sondern auch die Drahtlose.

Als Beispiel hierfür gelten Reifendrucksensoren, diese sind komplett drahtlos angebunden und liefern einen Live-Status des Reifendrucks auf der Anzeige des Infotainments. Auch die Kommunikation zwischen Fahrzeugschlüssel und Türen des Fahrzeugs und die Wegfahrsperre erfolgen drahtlos.[12] Hierfür werden RFID-Kennungen (Radio Frequency Identification) in der Fernbedienung zum Ver- und Entriegeln der Türen verbaut. Die Menge an produzierenden Daten, die dabei entstehen belaufen sich auf 10-25 GB die Stunde. Diese werden durch die Ausstattung des Autos mit ca. 40 Mikroprozessoren generiert, die ständig weitere Daten von Sensoren auswerten. Diese Daten werden wie bei Smartphones von dem Fahrzeug selbst abgerufen. Dazu zählen auch die einzelnen Komponenten, die im Fahrzeug verbaut sind, dies geschieht durch die Abfrage der VIN (Vehicle Identification Number), also einer Fahrzeugidentifikationsnummer, welche jedes Fahrzeug individuell besitzt. Die Abfrage der VIN geschieht durch eine sogenannte OBD-II-Schnittstelle.[13]

[11] Vgl. Raith, N. 2019, S. 15 (online, URL siehe Literaturverzeichnis).

[12] Vgl. Krauß, C./Waidner, M. 2015, S. 384.

[13] Vgl. Hansen, M. 2015, S. 367.

OBD steht für die On-Board-Diagnose-Dose und ist eine physikalische Schnittstelle, die innerhalb des Fahrzeugs liegt. Sie dient zur Auslesung von Fahrzeugdaten durch ein externes Diagnosetool, welche sich von Hersteller zu Hersteller unterscheiden. Die Fahrzeugdaten werden über eine Diagnoseschnittstelle eines Datenbusses ausgelesen, um die gespeicherten Fehler des Steuergeräts nachvollziehen zu können. Nach aktuellem Stand der Technik wird nur die Kilometerzahl des Fehlers gespeichert, jedoch nicht die Uhrzeit. Entwickelt wurde die OBD-II-Schnittstelle zur Datenabfrage von Relevanten Informationen bzgl. Emissionen. Mittlerweile können auch Reparaturdaten und Wartungsdaten des Fahrzeugs hieraus gefiltert werden. Die Schnittstelle wird heutzutage auch für Unfallereignisse ausgelesen, da durch das Auslesen der Unfall rekonstruiert werden kann und somit viele neue Informationen daraus gewonnen werden.[14] Des Weiteren ist die OBD-II-Schnittstelle nicht nur für die Rekonstruktion für Unfälle entwickelt wurden, sondern auch für die Qualitätssicherung und Qualitätsverbesserung von zukünftigen Fahrzeugmodellen. Die hieraus gewonnenen Daten sind auch für Versicherungen von enormer Bedeutung, da sie durch die Auswertung des Fahrverhaltens individuelle Versicherungstarife anbieten können und somit ihren Markt mit der Strategie des „Pay as you drive“, also “zahlen Sie, während Sie fahren”, verwirklichen.[15]

Eine weitere Basisschnittstelle im Fahrzeug, wie oben bereits kurz erwähnt, ist das sogenannte CAN-Bussystem, welches aktuell zu dem am häufigsten eingesetzten Kfz-Bussystemen zählt und einen echtzeitfähigen Feldbus für serielle Datenübertragungen darstellt.[16] Das System wurde in den 80er Jahren von der Firma Bosch entwickelt und gewinnt nicht zuletzt durch ihre Standardisierung mittels ISO-Normen (Internationale Standardisierungs Organisation) in der Automatisierungstechnik an Bedeutung. In der Automobilindustrie wird es primär für die Vernetzung der Steuergeräte, wie in Abbildung 1 zu sehen ist, eingesetzt.

[14] Vgl. Raith, N. 2019, S. 13 ff. (online, URL siehe Literaturverzeichnis).

[15] Vgl. Krauß, C./Waidner, M. 2015, S. 383.

[16] Vgl. Zimmermann, W./Schmidgall, R. 2007, S. 32 ff.

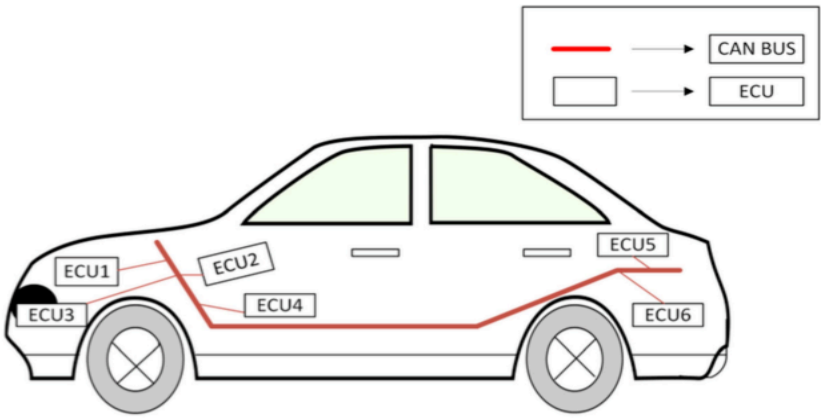

Abbildung 1. Bussystem im Automobil [17]ECU (zu Deutsch: Steuergerät)

Innerhalb des Systems werden die Geschwindigkeiten des Datentransfers von einem Steuergerät zum anderen unterteilt. Die Datentransferraten sind vor allem von der Kabellänge abhängig, so beträgt die Geschwindigkeit bei 40 Metern in etwa 1 Mbit/s, bei einem Kilometer, ohne zusätzliche Empfangsverstärker wie Repeater oder Bridges, nur noch 80 kbit/s. Der CAN-B ist für die langsamere Datengeschwindigkeit konzipiert wurden. Dieser wird vor allem in der Karosserie- und Fahrzeugelektronik eingesetzt und erreicht Geschwindigkeit bis zu 83,33 kbit/s. Für die Antriebs- und Fahrwerkselektronik wird das CAN-C eingesetzt, welches Datenraten bis zu 500 kbit/s bewerkstelligen kann.[18]

2.2.2 Externe Kommunikationssysteme

Um die externen Kommunikationssysteme des Fahrzeugs besser zu verstehen, muss vorher das Internet of Things im Sinne des vernetzten Automobils näher erläutert werden. Unter der Kategorie der „Dinge“ sind Komponenten gemeint, wie die Fahrzeugverbindung zu den Automobilherstellern und den Händlern. Auch die Kommunikation mit den Regierungsbehörden bzgl. Mautstellen, die Verbindung der Infrastruktur mit dem Fahrzeug wie z.B. mit Ampeln oder Parkhäusern und die Verbindung eines Fahrzeugs mit einem anderen Fahrzeug sind wesentliche Aspekte des Internet of Things im vernetzten Automobil.[19]

---

[17] Vgl. Islam, R./Refat, R.U.D. 2020.

[18] Vgl. CAN-Bussysteme ITWissen 2020h (online, URL siehe Literaturverzeichnis).

[19] Vgl. Johanning, V./Mildner, R. 2015, S. 8.

So wird im Prozessverlauf der Konnektivität nicht nur die Internetfähigkeit angestrebt, sondern noch viele weitere Kommunikationsmodelle in das Automobil integriert. Es wird von Modellen des „Car2X“ gesprochen, wobei das „X“ eine flexible Variable ist, welche beispielsweise für die Infrastruktur stehen kann.[20] Diese Kommunikationsmodelle können, wie bereits erwähnt, eine Art Vorstufe des autonomen Fahrens darstellen und werden im Folgenden näher erläutert.

Car2Car-Kommunikation:

Bei der Car2Car-Kommunikation oder auch Car-to-Car (abgekürzt C2C), wird sich vor allem mit der Thematik des direkten Informationsaustausches zwischen sich bewegenden Fahrzeugen beschäftigt. Durch die C2C-Kommunikation soll frühestmöglich dem Fahrer angezeigt werden, dass ein Unfall droht oder sich ungewöhnliche Hindernisse auf der Fahrbahn befinden. Weiterhin soll der Verkehrsfluss durch die vorzeitige Warnung vor Staus, auch ohne Sichtkontakt zu anderen Fahrzeugen, zur Optimierung der Straßensicherheit beitragen.

Die Fahrzeuge können sich mit dem C2C gegenseitig vor Unwetterverhältnissen wie Aquaplaning oder Blitzeis warnen und tragen zusätzlich der Vision Zero bei. Aber nicht nur der Informationsaustausch der Fahrzeuge bezüglich der Unwetterverhältnisse ist ein Thema bei der C2C, sondern auch die frühzeitige Gefahrenwarnung. Ein ABS wird beispielsweise durch die Verbindung des Internets mit den Elektronik- bzw. Elektriksensoren des Autos gekoppelt, um so nachfolgende Autos über die Gefahr, wie z.B. Kinder die einem Ball hinterherlaufen, per Internet zu informieren. Das C2C Konzept soll die allgemeine Sicherheit im Straßenverkehr erhöhen und diese zeitgleich intelligenter organisieren, was folglich den kompletten Straßenverkehr nachhaltiger ablaufen lässt.[21]

[20] Vgl. ebenda, S. 15.

[21] Vgl. Elektronik-Kompendium 2020a (online, URL siehe Literaturverzeichnis).

Car2Infrastructure-Kommunikation:

Anders als die C2C-Kommunikation kommuniziert das Fahrzeug bei der Car2Infrastructure (abgekürzt C2I) mit Infrakstruktureinrichtungen wie beispielsweise Ampelsystemen. Dieses Prinzip erschafft neue Geschäftsmodelle wie z.B. das bereits vorgestellte Versicherungskonzept des „pay as you drive“, dass bei der C2I ihren Ursprung findet. Einige Parkhäuser in Deutschland bieten mittlerweile das System der freien Parkplatzsuche an. Hier sind die Parkhäuser so ausgestattet, dass sobald eine Parklücke frei wird, eine grüne Birne aufleuchtet, damit der Fahrer Bescheid weiß, dass ein freier Platz vorliegt. Sind Parklücken besetzt, leuchtet die Lampe rot auf. Nach diesem System arbeitet auch das C2I für die automatische freie Parkplatzsuche. Viele Automobilhersteller bieten diesbezüglich schon das komplett automatische Parken an. Genau wie bei dem Modell des C2C zielt das C2I ebenfalls auf die Optimierung des Verkehrsgeschehens ab.

Durch das frühe Erkennen von Ampelphasen, intelligenter Verkehrsschilderkennung und die Herausgabe von Informationen über Staus soll das System zur Optimierung beitragen.[22] Insgesamt soll das System dem Sicherheitskonzept beitragen, indem sicherheitsspezifische Informationen durch Sensordaten erfasst werden. Diese können Aufschluss darüber geben, inwiefern das Sichtfeld durch Nebel oder Feuchtigkeit beeinträchtigt wird. Außerdem erhalten Fahrer Warnungen bzw. Informationen, wenn sich Notfallautos nähern, um folglich eine ordnungsgemäße Rettungsgasse bilden zu können, die häufig über Leben und Tod entscheidet.[23]

Car2Enterprise:

Abzugrenzen ist das Car2Enterprise (abgekürzt C2E) von dem C2I. Hierbei geht es um Kommunikation des Fahrzeugs mit Infrastrukturen, die privatwirtschaftlich und kommerziell betrieben werden. Hierzu zählen Infrastrukturen wie Hotels, Parkhäuser oder auch Tankstellen. Wird von einer Kommunikation eines Fahrzeugs mit dem Parkhaus ausgegangen, kann das Fahrzeug überprüfen, ob generell ein freier Parkplatz im Parkhaus vorhanden ist, ohne vorher in dieses hinein gefahren zu sein. Das Fahrzeug kann somit zu einer freien Parklücke per Navigation hingeführt werden.

---

[22] Vgl. IT-Wissen 2020b (online, URL siehe Literaturverzeichnis).

[23] Vgl. Johanning, V./Mildner, R. 2015, S. 15 ff.

Auch das Bezahlsystem findet automatisch mit dem Parkhaus statt, da genauestens überprüft werden kann, wie lange ein bestimmtes Fahrzeug in dem Parkhaus geparkt hat.[24]

Car2Home-Kommunikation:

Bei diesem Kommunikationstypus liegt der Fokus auf dem Komfort des Fahrzeugbesitzers. Bei dem Car2Home (abgekürzt C2H) entsteht eine Verbindung des Fahrzeugs mit dem eigenen Zuhause. Hierbei sind Medien wie Hörbücher, Streamingdienste oder Filme per Vernetzung des Autos abrufbar. Vorstellbar sind Szenarien wie die Einstellung der Navigationsroute von der heimischen Couch aus und anschließend das Abrufen der Route im Fahrzeug.[25]

Automobilhersteller bieten die Funktion eines Online-Fahrtenbuches an, um genauestens nachverfolgen zu können, welche Fahrt wann angetreten wurde. Auch kann von Zuhause bequem per App der Zustand des Fahrzeugs erfragt werden. Hierzu zählen Informationen wie der Tank- oder Ölstand. Fast alle Automobilhersteller bieten zudem noch die Sonderausstattung der per App bedienbaren Klimaanlage an. So kann von außerhalb des Fahrzeugs die Klimaanlage auf die gewünschte Temperatur voreingestellt werden.[26]

Die folgende Abbildung 2 zeigt die in Kapitel 2.2.1 und 2.2.2 genannten internen und externen Systeme des Automobils auf und fasst die bestehenden IT-Komplexität zusammen. Die Systeme werden hierbei in drei Ebenen unterteilt: Netzwerkebene, Backend- und Cloudebene sowie Fahrzeugebene.

[24] Vgl. ebenda, S. 16.

[25] Vgl. Sänn, A. et al. 2017, S. 61 ff.

[26] Vgl. Johanning, V./Mildner, R. 2015, S. 16.

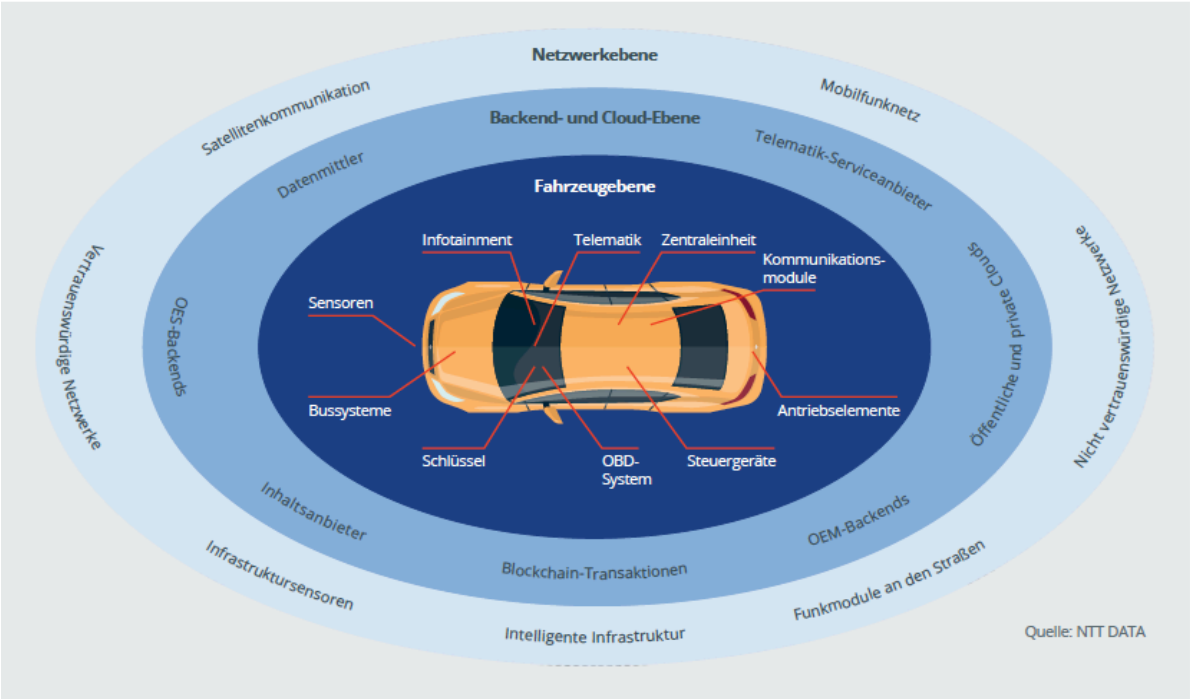

Abbildung 2. Fahrzeugsysteme im vernetzten Automobil[27]

3. Automobile Sicherheitsarchitektur

3.1 Elemente der Fahrzeugsicherheit

Die zunehmende Verflechtung interner sowie externer Fahrzeugsysteme steigert, analog zur IT-Komplexität der Implementierung, die Gefahr von Fehlfunktionen und das Versagen von Schutzmaßnahmen im vernetzten Automobil. Folglich kann es zu Systemausfällen, Verlust von Daten bis hin zur unberechtigten Übernahme des Fahrzeugs kommen. Standardisierte Prozesse und Normen sollen bereits in der Entwurfsphase neuer Systeme das Fehlerpotenzial einschränken, sodass das Risiko gemindert wird neue Gefahren in das Fahrzeug einzubauen.

Dementsprechend ist eine nachträgliche Implementierung der Konzeption aus folgenden Gründen nicht ratsam: Die Kosten und Personalressourcen, die bei der Identifikation, beim Entwurf und letztlich bei der Umsetzung für die Absicherung von sicherheitsrelevanten Maßnahmen der elektronischen Steuerungssysteme entstehen, können für andere kosten- und zeitintensive Einheiten effizienter genutzt werden.

[27] Vgl. Cybersecurity Roadmap 2020d, S. 2 (online, URL siehe Literaturverzeichnis).

Bei der späteren Realisierung kann es weiterhin auch zu falschen Anweisungen kommen, die evtl. nicht für Schutz sorgen, sondern eine neue Schwachstelle ergeben, welche sich kontraproduktiv z.B. bei einem späteren Angriff auswirken kann. Gleiches gilt auch für die unvollständigen oder inkonsistenten Maßnahmen gegenüber dem Zugriff von Dritten. Schließlich können bei der nachträglichen Implementierung zusätzlich unabsichtliche Schwachstellen eingefügt werden, die wiederum nicht im Sinne der Cybersecurity produktiv wären.[28]

Die Komplexität des Entwicklungsansatzes zeigt bereits Widersprüche innerhalb der Begrifflichkeiten Cybersecurity, funktionale Sicherheit und Schutz personenbezogener Daten auf. Folglich gilt es als übergeordnetes Ziel eines OEM die verschiedenen Elemente in Einklang zu bringen. Hierbei kommt es allerdings zu einem Spannungsverhältnis der drei Akteure, welches mithilfe des magischen Dreiecks symbolisiert werden kann:

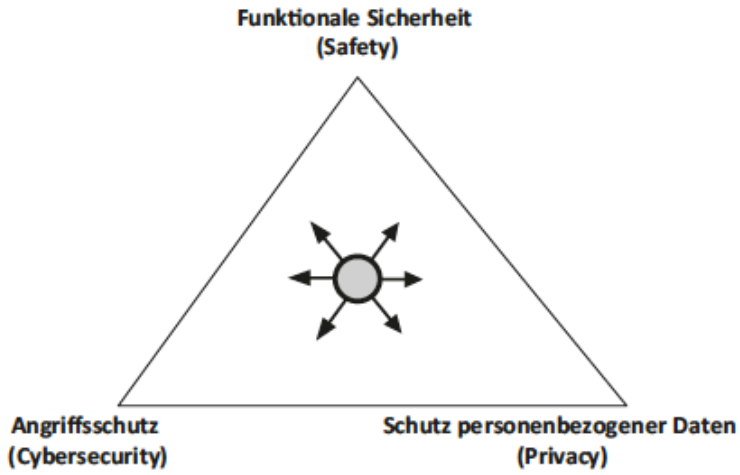

Abbildung 3. Spannungsverhältnis im magischen Dreieck[29]

Das erste Problem zeigt sich bereits in der Einigung, die Datenverarbeitung auf geringe Latenzzeiten zu beschränken und im gleichen Zuge ein datenintensives Abwehrsystem mittels verschlüsselter Kryptografie in das Fahrzeug zu integrieren.

---

[28] Vgl. Schnieder, L./Hosse, R.S. 2018, S. 5.

[29] Vgl. ebenda, S. 4.

Dieses gilt es zusätzlich über die Verknüpfung zu externen Fahrzeugsystemen zu erweitern. Dieser Optimierungsansatz der Cybersecurity steht jedoch im negativen Verhältnis zum Schutz personenbezogener Daten, da die eigenen Fahrzeugdaten transparent gemacht werden. Vervollständigt wird das Dilemma durch das Tracking und Profiling der Fahrdaten: Hier steht der Nutzen der funktionalen Sicherheit im Widerspruch zur Steigerung des potenziellen Datenmissbrauchs der personenbezogenen Daten.[30]

Um einen umfassenden Entwicklungsansatz für das Automobil zu konzipieren, gilt es für jedes der drei Sicherheitselemente ein strukturiertes Konzept zu entwickeln. Funktionale Sicherheit entspricht dem Schutz vor systematischen und zufälligen Ausfällen des Automobils an sich. Der Datenschutz umfasst die Verschlüsselung jeglicher Fahrerdaten sowie Kommunikationsdaten. Cybersecurity beschreibt hierbei Maßnahmen, die zur Abwehr eines unberechtigten Eingriffs nötig sind, der den Schutz des Steuerungssystems negativ beeinflusst. Einschränkend wird bei den Sicherheitsmaßnahmen von Wahrscheinlichkeiten der Risikominderung gesprochen, um der Gewährleistung von absoluter Sicherheit zu umgehen. Basierend auf der ISO 26262 leitet sich daraus der Engineering-Prozess zur Erreichung maximaler Cybersecurity, aber auch funktionaler Sicherheit ab, bei dem zunächst der Entwurf angriffssicherer Systeme und anschließend die Eigenschaftsabsicherung der identifizierten Systeme vorgenommen wird.[31]

3.1.1 Funktionale Sicherheit

Um eine Grundqualität in allen Entwicklungsaktivitäten des Automobils zu gewährleisten müssen gewisse Industriestandards in der Herstellung vorgewiesen werden. Dabei zählen zu der Einhaltung funktionaler Sicherheit die Bestimmungen des Automotive SPICE (Software Process Improvement and Capability Evaluation) und der ISO 26262, welche wiederum an der Passung des SPICE-Standards ansetzten und die Grundvoraussetzungen des Cybersecurity-Ansatzes liefert.[32]

---

[30] Vgl. ebenda, S. 4 ff.

[31] Vgl. Johanning, V./Mildner, R. 2015, S. 79; Vgl. Schnieder, L./Hosse, R.S. 2018, S. 2.

[32] Vgl. Johanning, V./Mildner, R. 2015, S. 86.

Der Industriestandard Automotive SPICE bewertet die Reife von Systementwicklungsprozessen. Der Standard ist ein Warenzeichen der Volkswagen AG und wird häufig auch “ASPICE” genannt. Als Schwerpunkt im ASPICE Modell wird die Software behandelt. Die Bewertung erfolgt auf Grundlage des 2007 festgelegten internationalen Standards der ISO 15504, wobei ASPICE eine grundlegende Teilmenge der dort definierten Prozesse bildet. Der Standard beinhaltet einen Fragenkatalog, der die Reife der Prozesse in sechs Stufen untergliedert:[33]

Reifegrad 0: unvollständig. Die Arbeit der Entwicklungsorganisation wird als nicht systematisch eingestuft und geforderte Produkte können höchstens mit viel Glück erzielt werden.

Reifegrad 1: durchgeführt. Zwar werden gewisse Arbeitsergebnisse der Entwicklungsorganisation geliefert, dennoch sind diese weder systematisch durchgeplant, noch in konstanter Qualität vorliegend.

Reifegrad 2: gesteuert. Die Arbeit der Entwicklungsorganisation liefert wie geplant, allerdings liegen noch Probleme in speziellen Projektarten und Sonderfällen vor. Weiterhin ist eine einheitliche Arbeit nicht erkennbar.

Reifegrad 3: etabliert. Die Arbeit der Entwicklungsorganisation ist hinsichtlich ihrer Prozesse definiert und klar dokumentiert. Außerdem sind Lösungen für spezielle Probleme konzipiert.

Reifegrad 4: vorhersagbar. Die Arbeit der Entwicklungsorganisation erfüllt die geforderten Leistungsfähigkeiten der einzelnen Prozessschritte und das dazugehörige Kontrollmanagement besteht.

Reifegrad 5: optimierend. Die Arbeit der Entwicklungsorganisation sticht durch die Planung und ihre kontinuierliche Verbesserung hervor. Die Arbeit verläuft nach Plan.[34]

---

[33] Vgl. Horváth, P./Seiter, M. 2012, S. 34 ff.

[34] Vgl. Johanning, V./Mildner, R. 2015, S. 79 ff.

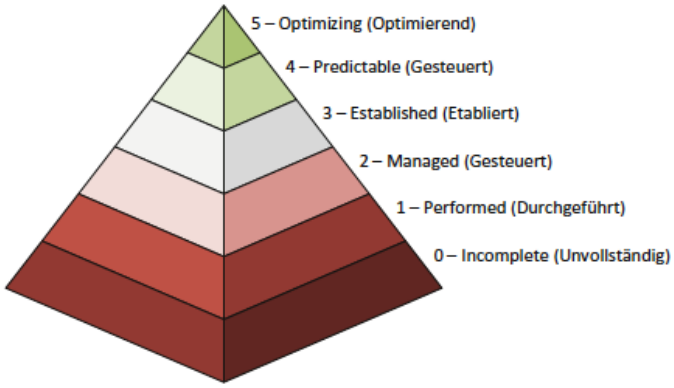

Abbildung 4. Reifegrade gemäß Automotive SPICE[35]

Die bereits mehrfach erwähnte ISO 26262 für die funktionale Sicherheit (FuSi-Standard) stellt einen Standard für sicherheitsrelevante Industrien dar. Darunter zählt auch der im Jahre 2011 eingeführte Standard für die Automobilindustrie. Anders als den Automotive SPICE-Standard, der sich aktuell gänzlich mit der Software auseinandersetzt, setzt sich der FuSi-Standard sowohl mit der Software als auch mit der Hardware auseinander. Hierfür definierte der FuSi-Standard ein Handbuch für die Risikoanalyse und -vermeidung, dessen Umfang durch den Automotive Safety Integrity Level (ASIL) determiniert wird. Dieser beschäftigt sich mit den zu ergreifenden Maßnahmen gegen systematische Fehler und Ausfälle. Im Rahmen eines Assessments gibt es folgende Kriterien zur Bewertung der elektronischen Lenkung:

Eintrittswahrscheinlichkeit (Exposure, “E”): Beschreibt die Häufigkeit der Fahrsituation, in denen potentielle Fehlfunktionen sicherheitsrelevant sein können. Als Beispiel wird folgende kritische Betriebssituation genannt: Bei hohen Geschwindigkeiten und großen Kurvenradien, ist die Unterstützung für den Fahrer gering, wie es bei Autobahnfahrten üblich ist.

[35] Vgl. ebenda, S. 82.

Beherrschbarkeit (Controllability, “C”): Beschreibt den potenziellen Schadensausmaß. Wie bei der zuvor geschilderten kritischen Betriebssituation auf Autobahnen, kann das Fahrzeug unerwartet einen engeren Kurvenradius einschlagen. Dies kann zu Kollisionen mit anderen Fahrzeugen, Passanten und der Infrastruktur führen und potenziell tödlich enden.

Schwere des Fehlers (Severity, “S”): Beschreibt die Bewertung der Kontrollierbarkeit. Als Worst Case könnte die elektronische Lenkung unerwartet maximal mögliche Unterstützung leisten, was wiederum für den Fahrer, aufgrund der hohen Geschwindigkeit auf Autobahnen, nicht zu bewerkstelligen ist. Dem Fahrer steht somit nur eine geringe Reaktionszeit zur Verfügung. Die Fehlfunktion “Unterstützung zu stark” kann somit zur Gefährdung des “Selbstlenkens” führen und muss, um die Gefährdung der elektronischen Lenkung mit den Parametern der Häufigkeit, Kontrollierbarkeit und Schadensschwere gemäß des ASIL realisiert werden.[36]

Die funktionale Sicherheit wird im Gesamtkontext des Sicherheitskontrukts des vernetzten Automobils betrachtet und die beschriebenen Vorstufen als theoretische Pflicht-Grundlage angesehen. Jedoch liegt der spätere Fokus, auch unter dem Aspekt der nachfolgenden Anwendung der Modelle, auf den Themengebieten der Cybersecurity und Kryptografie.

3.1.2 Cybersecurity

Aufbauend auf der funktionalen Sicherheit und der Norm ISO 26262 leitet die Cybersecurity ihren systematischen Engineeringansatz ab, um die Anzahlmöglichkeiten externer Zugriffe auf ein Minimum zu beschränken.[37] Zunächst erfolgt der Schritt der Feature Definition, welche die Eingrenzung des Betrachtungsgegenstandes beschreibt. Hierbei erfolgt bei der Systementwicklung eine möglichst präzise Definition des zu entwickelnden Systems. Dieses Verfahren soll sich dem Entwicklungsprozess der Cybersecurity unterwerfen, wobei die physikalischen Grenzen des Systems bestimmt und die zu schützende Bereiche aufgezeigt werden.

---

[36] Vgl. Schnieder, L./Hosse, R.S. 2018, S. 1 ff.; Vgl. Johanning, V./Mildner, R. 2015, S. 83 ff.

[37] Vgl. Schnieder, L./Hosse, R.S. 2018, S. 13.

Dabei wird im Betrachtungsumfang der Zusammenhang zwischen sicherheitsrelevanten elektronischen Steuerungssystemen für KFZ und den Cybersecurity-Systemen festgelegt, welche Analysen hierfür getätigt werden müssen und was es zu beachten gibt. Besonders im Fokus stehen hierbei die Zugriffe und Attacken unberechtigter Dritter. Alle Steuerungssysteme müssen davor geschützt sein, da ein unberechtigter Zugriff oder eine Attacke verheerende Auswirkungen haben kann und somit relevante Sicherheitsziele scheitern lässt. Jedoch gilt es diese Sicherheitsziele unterschiedlich zu priorisieren, da die Attacken verschiedene Schweregrade zur Folge haben. So wird beispielsweise zwischen dem Scheitern der Zielerreichung an sich und der Ingefahrbringung des Insassen unterschieden. Dabei wird erneut das Dilemma zwischen den Ecken des magischen Dreiecks symbolisiert.[38]

Grundlegend besteht das Konstrukt des Cybersecurity-Engineering aus der Bestimmung der Bedrohungsidentifikation, zur Konstitution der potenziellen Angriffe, und der Risikobewertung, zur Priorisierung der Attacken. Die Schritte der Bedrohungsidentifikation sowie die Maßnahmen der Risikobewertung (Threat Analysis and Risk Assessment, kurz: TARA) werden grundlegend anhand der Feature Definition durchgeführt. Die TARA wird zur Identifikation von Gefährdungen genutzt. Sie bewertet außerdem das Risiko sowie das Restrisiko der zuvor identifizierten Bedrohung. Die TARA-Ergebnisse werden gesammelt und umfassen die weitere Konstruktion der Aktivitäten.[39]

1. **Identifikation von Bedrohungen:**
   Bei der Identifizierung von Bedrohungen kommt grundsätzlich eine Methode zum Einsatz: STRIDE. Microsoft stellte hierzu erstmalig das STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) Klassifikationsmodell vor. Das STRIDE Modell ist eine strukturierte, qualitative Analysemethode, die mögliche Bedrohungen vollständig erfassen soll. So wird jeder Bedrohungskategorie ein Security-Attribut zugeordnet und leitet insgesamt eine Cybersecurity-Anforderung ab.

[38] Vgl. Schnieder, L./Hosse, R.S. 2018, S. 13 ff.

[39] Vgl. Huber, E. 2015, S. 92 ff.

Im Beispiel der Bedrohung durch Spoofing, wobei der Angreifer vorgibt jemand anderes oder etwas anderes zu sein, wäre das gewünschte Attribut dementsprechend die Authentizität.

Angewendet wird die Methode mithilfe von sogenannten Attack Trees (zu Deutsch: Bedrohungsbäume). In einem Attack Tree werden alle Bedrohungen vollständig erfasst und anschaulich dargestellt. Der Attack Tree startet in der Regel oben an der Wurzel mit dem Angriffsziel, also der Bedrohung des Systems. Die Kinder des Knotens stehen für die Zwischenziele, die zur Erreichung des Ziels des Vaterknotens dienen. Die Zwischenziele werden mit einem logischen UND beziehungsweise einem ODER miteinander verknüpft. Bei der UND Beziehung müssen alle Bedrohungen vorliegen, damit die Bedrohung des Vaterknotens eintritt. Bei der ODER Beziehung hingegen muss hierfür nur eines der Zwischenziele eintreten. Der Pfad von einem Blatt zur Wurzel repräsentiert die Schritte, die zur Erreichung des in der Wurzel definierten Angriffsziels liegen.

2. Risikobewertung

Sobald die Bedrohung gemäß der Beschreibung identifiziert ist, können die Risiken mit verschiedensten Methoden bewertet werden. Zum einen wird die Wahrscheinlichkeit des Zugriffs betrachtet und zum anderen der voraussichtliche Schweregrad des Schadens bewertet.

Ein weit verbreitetes Modell zur Bewertung der Wahrscheinlichkeit eines Zugriffs ist HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safety), indem insgesamt vier Kriterien valutiert werden: Fachwissen, Systemwissen, Ausrüstung und Zugriffsmöglichkeit. Ein gewisses Maß an Fachwissen der grundlegenden Prinzipien, Produktkategorien und Angriffsmethoden wird für einen erfolgreichen Angriff vorausgesetzt. Die Verfügbarkeit von Informationen zum System und der Größe der Community sind wichtige Bestandteile des Systemwissens. Daraus lässt sich ableiten, ob ein Angriff als schwer oder leicht eingestuft werden kann.

Für einen erfolgreichen Angriff müssen genügend Ressourcen vorhanden sein, damit im Vorhinein die Schwachstellen identifiziert werden können, um sie anschließend auszunutzen. Bei der Zugriffsmöglichkeit wird zusätzlich der Zugriffstyp und die Zeitdauer bewertet. Bei den Zugriffstypen handelt es sich um das logische oder physische Angriffsziel. Die Dauer bestimmt, wie viel Zeit für einen Angriff in Anspruch genommen werden kann.

Zur Bewertung des Schadensausmaßes eines unbefugten Zugriffs nach HEAVENS wird dieser mittels verschiedener Schweregrade bewertet. Dazu erfolgt die Unterteilung in vier weitere Kategorien: finanzielle Auswirkung, Komfort- und Verfügbarkeitseinschränkungen, Verlust der Vertraulichkeit und Sicherheitsrelevanz. Dabei kann innerhalb dieser Klassen in Form von verhängten Geldbußen, Beeinträchtigung von nicht sicherheitsrelevanten Systemen, Datenmissbrauch und der Garantie der funktionalen Sicherheit des OEMs unterschieden werden.

Die beschriebenen Kategorien des Schweregrades und der Wahrscheinlichkeit des Schadens werden in einer Risikomatrix miteinander verknüpft. Daraus resultieren die Schutzgrade zur Erreichung eines angemessenen Schutzniveaus. Das Schutzniveau definiert die Häufigkeit und Schwere eines aus einer Bedrohung resultierenden Schadens. Die Matrizen dienen zur Erreichung des Schutzniveaus durch die gezielte Maßnahmenauswahl, wobei solche Matrizen nicht nur in der Automobilindustrie immer mehr an Bedeutung gewinnen.[40]

Mit den identifizierten TARA-Ergebnissen erfolgt die Ableitung von allgemeinen Cybersecurity-Zielen. Diese bestimmen für jede mögliche Bedrohung, mit dem zugehörigem Restrisiko, was es zu vermeiden bzw. zu erkennen gilt. So kann die Verhinderung eines externen, unerlaubten Zugriffs als beispielhaftes Cybersecurity-Ziel gesehen werden.

[40] Vgl. Schnieder, L./Hosse, R.S. 2018, S. 14 ff.

Abstrahiert man diese Formulierungen weiter, ergibt sich das Cybersecurity-Konzept, welches die Erreichung der Ziele beschreibt. In Kombination ergeben die beiden strategischen Maßnahmen die notwendigen Erkenntnisse zur Bestimmung der funktionalen Cybersecurity.[41]

3.1.3 Datenschutz und Kryptographie

Der dritte Aspekt des magischen Dreiecks umfasst den Schutz der durch die Vernetzung neu aufkommende Datenmenge und deren Verschlüsselung mittels verschiedener Verfahrensmöglichkeiten. Durch den Komplex der Car-2-X Kommunikation werden Unmengen an Daten in den Umlauf gebracht. Dabei werden die Daten von Hersteller zu Hersteller unterschiedlich realisiert und gehandhabt, teilweise unterscheiden sich die Umsetzungen bereits innerhalb der Ausstattungsvarianten und Modellreihen. Die Daten die erzeugt, verarbeitet, gespeichert und weitergeleitet werden, werden in Datenkategorien eingeordnet. Betriebsdaten, Komfortfunktionsdaten, Fehler- bzw. Wartungsdaten, Unfalldaten und vom Fahrer erstellte Daten sind typisch gespeicherte Werte. Allerdings lassen sich diese Kategorien zumeist kaum voneinander trennen, da z.B. Fakten, die bei der Inbetriebnahme des Fahrzeugs entstehen, wie z.B. die Geschwindigkeit, auch für die Daten der Komfortfunktionen, wie der Positionsbestimmung im Tunnel, genutzt werden.[42]

Zu den Betriebsdaten die ständig vom Fahrzeug erfasst werden, gehören Informationen wie die Motortemperatur, Reifenluftdruck, Kraftstoff-/ Ladezustand, aktuelle Geschwindigkeiten, Radumdrehungen oder auch die Lebensdauer des Motoröls. Die meisten der aufgelisteten Betriebsdaten werden im fest verbauten Kombiinstrument des Fahrzeugs angezeigt. Die Werte werden während der Fahrt ständig aktualisiert und flüchtig gespeichert; wird das Fahrzeug ausgeschaltet, werden die Daten gelöscht. Allerdings erfolgt bei einigen Daten die Langzeitspeicherung, diese werden erst über die oben beschriebene OBD-II-Schnittstelle zurückgesetzt, wie z.B. Wartungsdaten oder Lebensdauer des Motoröls.

---

[41] Vgl. ebenda, S. 19 ff.

[42] Vgl. Hansen, M. 2015.

Bei den Komfort- und Sicherheitsfunktionsdaten werden viele Angaben von außerhalb mittels Sensoren erfasst, ähnlich dem Prinzip der Car2X-Kommunikation. Zu den typischen Funktionen zählen: Außentemperaturanzeige, Rückfahrkamera, automatische Abstandshaltung, Spurhalteassistent oder auch Gefahrenwarnungen. Diese Art von Daten wird zu meist flüchtig gespeichert und spätestens mit dem Abstellen des Fahrzeugs wieder gelöscht. Wie zuvor bei den Betriebsdaten werden jedoch bestimmte Informationen über einen längeren Zeitraum gespeichert, so z.B. die Daten der Fahrweisen, um das Nutzungsverhalten anzupassen und zu verbessern.

Fehler- und Wartungsdaten hingegen werden generell über einen längeren Zeitraum gespeichert. Hierbei werden im Steuergerät zu bestimmten Ereignissen, wie beispielsweise einer erhöhten Motordrehzahl, ein Fehlercode erzeugt, der zusammen mit dem Kilometerstand, Datum und Uhrzeit gespeichert wird. Fehlerdaten zu Wartungszwecken werden bis zum nächsten Termin bei der Werkstatt gespeichert. Werden Grenzwerte überschritten, zeigt das Kombiinstrument eine Warnung an, dass demnächst eine Wartung stattfinden sollte und ggf. Teile ausgetauscht werden müssen.

Im Falle eines Unfalls werden Zeitpunkt oder die aktuelle Querbeschleunigung im Airbag-Steuergerät in einem speziellen Unfalldatenspeicher aufgenommen. Bei vorhandenem eCall-System werden die Werte direkt an die Notrufzentrale weitergeleitet.[43]

Im Fahrzeug werden jedoch nicht nur die Daten gespeichert, die von dem Fahrzeug selbständig erfasst oder von externen Dritten bereitgestellt werden, sondern auch die Informationen, die der Insasse selbst eingebracht hat. Das können beispielsweise Infotainment-Daten wie Kontakte, Adressen oder Telefonnummern sein, aber auch Daten wie Navigationsziele, Radiosender- und Klimaanlageneinstellungen. Diese Informationen werden manuell in den jeweiligen Steuergeräten bis hin zur Löschung gespeichert.

[43] Vgl. Krauß, C./Waidner, M. 2015.

Durch spezifische Apps, der Head Unit, über das Kombiinstrument verkoppelte mobile Endgeräte oder über die OBD-II-Schnittstelle kann auf die Daten zugegriffen werden.[44]

Bei der aufgezeigten und dabei nur beispielhaften, angerissenen Menge an Daten, liegt das Thema des Datenmissbrauchs nahe. Hier besteht sowohl bezüglich der Funktionssicherheit und der Datenschutzverletzungen viel Spielraum seitens der Hacker, aber auch systemeigene Fehler sind möglich. Ein Gesamtüberblick möglicher Bedrohungsarten wird in dem Kapitel 3.3 gegeben. Um die Relevanz kryptografischer Verfahren jedoch aufzuzeigen, werden hier Beispiele genannt.

Beginnend mit dem Auslesen persönlicher Fahrerdaten, wie Geschwindigkeiten, Start- und Zielorte oder dem Fahrverhalten, wird bereits der gläserne Autofahrer geschaffen. Mittels dieser Bewegungsprofile kann zwischen den verschiedenen Fahrern differenziert werden. Vergleichsweise gefährlich kann der gezielte Einsatz von Malware werden, der ebenfalls den Zugriff auf die privaten Daten des Insassen gewährt. Die Möglichkeiten der Hacker weiter konzipiert, entwickelt sich aus dem Datenmissbrauch eine lebensbedrohliche Gefahr. Hier zeigt sich bereits: Analog zum Verflechtungsgrad der Assistenzsysteme und Datenmenge steigt die potenzielle Angriffsfläche des Automobils, welche es durch verschiedene Verschlüsselungs-Prinzipien vor der Außenwelt zu schützen gilt. Ein erster Ansatz bildet das Projekt QuantumRISC: Hierbei lautet das Ziel in Zukunft eingebettete Systeme des Autos mittels Kryptografie abzusichern und insbesondere einen Schutzstandard gegenüber Angriffen mit Quantencomputern zu liefern.[45]

In der PC-Welt haben sich bereits über Jahrzehnte kryptografische Verfahren bewiesen, diesen Erfolg gilt es nun auf die Automobil-Welt umzumünzen.[46] Das Projekt QuantumRISC entwickelt für diese Umstrukturierung sogenannte PQC-Verfahren (Post-Quantum-Cryptography), die den Sicherheitsanforderungen der Praxis gerecht werden sollen.

---

[44] Vgl. ebenda, S. 385.

[45] Vgl. Fraunhofer 2020e (online, URL siehe Literaturverzeichnis).

[46] Vgl. Genua 2020f (online, URL siehe Literaturverzeichnis).

Aktuelle PQC-Verfahren können allerdings aufgrund der hohen Rechenleistung und des hohen Speicherbedarfes nicht realisiert werden, da die eingebetteten Systeme im Fahrzeug momentan nicht über genügend Rechenleistung bzw. Speicherkapazität verfügen. Aus diesem Grund entwickelt das Projekt neue Verfahren, die gerade in solchen ressourcenbeschränkten Umgebungen ausreichend Schutz gewährleisten sollen. Dafür wird das Zusammenspiel der Anwendungsbereiche der Fahrzeugsysteme und Architekturen näher untersucht, um die Integration der hoch komplexen Kryptoverfahren zu ermöglichen.[47]

Wie bereits öfter in dieser Arbeit erwähnt, besitzt ein Fahrzeug eine Reihe an Software-Komponenten in den Steuergeräten. Diese gilt es gegen Manipulation von Software und Daten mittels digitaler Signaturen zu schützen.
So soll ein gewisser Schutzgrad ermöglicht werden, sodass eine Prüfung der digitalen Signaturen bereits vor einem Manipulations-Vorgang, auch Flash-Vorgang genannt, auf das Steuergerät den neuen Software Standard des autorisierten Herstellers entspricht und unverändert bleibt.[48]

Diese Prüfungen werden grundsätzlich mittels drei verschiedener kryptographischer Verfahren verschlüsselt. Um auf die Verfahren eingehen zu können, müssen zunächst Grundlagen geschaffen werden. Der Oberbegriff lautet Kryptologie, wobei sich dieser in die Untergebiete der Kryptografie und Kryptanalyse aufteilt. Die Kryptografie meint die Absicherung von Daten wie z.B. die Verschlüsselung, die Kryptanalyse beschäftigt sich hingegen mit dem Brechen von Kryptosystemen. Die Kryptanalyse ist heutzutage von enormer Bedeutung, da ohne sie nicht einzuschätzen wäre, ob ein kryptografischer Algorithmus als sicher einzustufen ist.[49]

[47] Vgl. Fraunhofer 2020e (online, URL siehe Literaturverzeichnis).

[48] Vgl. Elektroniknet 2020g (online, URL siehe Literaturverzeichnis).

[49] Vgl. Paar, C./Pelzl, J. 2016, S. 2.

Das erste Verfahren ist die symmetrische Verschlüsselung mit ihren symmetrischen Algorithmen, wobei dies die bekannteste Form der Kryptografie darstellt. Dies dient der Sicherstellung des Ziels der Vertraulichkeit und somit dem Ausschluss Dritter bei vom Abgreifen geheimer Daten.[50] Hierbei besitzen zwei Player eine Chiffre zum Ver- und Entschlüsseln mit der gemeinsamen Einigung eines geheimen Schlüssels, welcher nur in Besitz der beiden Player ist. Das Prinzip wird anhand eines Beispiels näher verdeutlicht. In der Literatur heißen die Player Alice und Bob, diese sind zwei Benutzer, die über einen unsicheren Kanal kommunizieren. Mit Kanal ist die Kommunikationsstrecke, wie beispielsweise das Internet, WLAN oder Mobilfunk, gemeint. Weiterhin gibt es einen Angreifer, der sich in der Literatur Oskar nennt, dieser erschafft sich einen Zugriff zum Kanal, über den Alice und Bob kommunizieren. Alice und Bob möchten selbstverständlich ihre Gespräche geheim halten, es könnte z.B. um Geschäftsstrategien gehen, wie zur Einführung eines neuen Fahrzeugmodells, wobei der Konkurrent, in diesem Fall Oskar, nicht mithören soll.

Hier kommt die symmetrische Kryptografie zum Einsatz: Die Nachricht von Alice wird mithilfe eines symmetrischen Verfahrens verschlüsselt und nennt sich in diesem Fall Variable x. Das Ergebnis der Verschlüsselung heißt das Chiffrat y. Dieses Chiffrat wird an Bob gesendet und von ihm entschlüsselt. Voraussetzung für diese Art der Verschlüsselung ist, dass der Verschlüsselungsalgorithmus so stark ist, dass Oskar durch reines Ausprobieren die Nachricht nicht entziffern kann.

Wichtig bei der Übertragung des Schlüssels ist die Kommunikation über einen sogenannten sicheren Kanal, der banal gesehen auch ein Zettel mit einem Code sein könnte. Genau dieses Prinzip des “pre-shared-keys” greift unser heutiges WLAN-Netzwerk auf. Wichtig zu erwähnen ist noch, dass die Ver- und Entschlüsselungsverfahren öffentlich gemacht werden müssen, da sie sonst nicht zu genüge auf Schwachstellen überprüft werden können und dies somit zugleich auch die einzige Möglichkeit darbietet, das Verfahren auf Schwachstellen zu testen. Das Verfahren muss somit öffentlich gemacht werden, allerdings nicht der Schlüssel, dies wäre kontraproduktiv und muss daher dringlichst geheim gehalten werden.[51]

---

[50] Vgl. Spitz, S. et al. 2011, S. 2.

[51] Vgl. Paar, C./Pelzl, J. 2016, S. 4 ff.

Diesen symmetrischen Ansatz verfolgte auch das amerikanische National Institute of Standard and Technology (NIST) bei ihrer Implementierung des AES (Advanced Encryption Standard) im Jahre 2001.[52] Das AES ist aktuell die meistgenutzte symmetrische Chiffre und wird für zahlreiche behördliche und industrielle Anwendungen als Standard vorgeschrieben, so auch in der Automobilwelt. AES verwendet Standards wie z.B. WLAN-Verschlüsselung IEEE 902.11i und Secure-Shell-Protokoll SSH.[53]

Das zweite Verfahren sind die asymmetrischen Algorithmen, auch Public-Key-Algorithmen genannt. Dieses Verfahren ist ähnlich dem Aufbau des symmetrischen Verfahrens, dient jedoch dem Schutz vor Manipulation von Daten und der Sendung falscher Informationen durch einen Dritten.[54] Auch soll die Möglichkeit abgewendet werden, dass sich ein Fremder für den wahren Bob oder die wahre Alice ausgibt und deren Identität fälscht.[55] Im Vergleich besitzt bei der symmetrischen Verschlüsselung ein Teilnehmer einen geheimen Schlüssel, der aber ebenso über einen öffentlich bekannten Schlüssel verfügt. So wird bei der symmetrischen Kryptografie derselbe geheime Schlüssel für die Ver- und Entschlüsselungen verwendet, wobei die Funktionen sich sehr ähneln. Um dies zu verdeutlichen, kommen wieder Alice und Bob ins Spiel: In einem Raum gibt es einen Safe mit einem starken Schloss, die Kopie des Schlüssels für das Schloss besitzen nur Alice und Bob. Der Safe dient dazu, die Nachrichten zu speichern, geöffnet werden kann dieser nur anhand des Schlüssels, den Alice und Bob besitzen.

[52] Vgl. Ernst, H. et al. 2020, S. 151 (online, URL siehe Literaturverzeichnis).

[53] Vgl. Paar, C./Pelzl, J. 2016, S. 103 ff.

[54] Vgl. Meinel, C./Sack, H. 2014, S. 15 ff. (online, URL siehe Literaturverzeichnis).

[55] Vgl. Küsters, R./Wilke, T. 2011, S. 190.

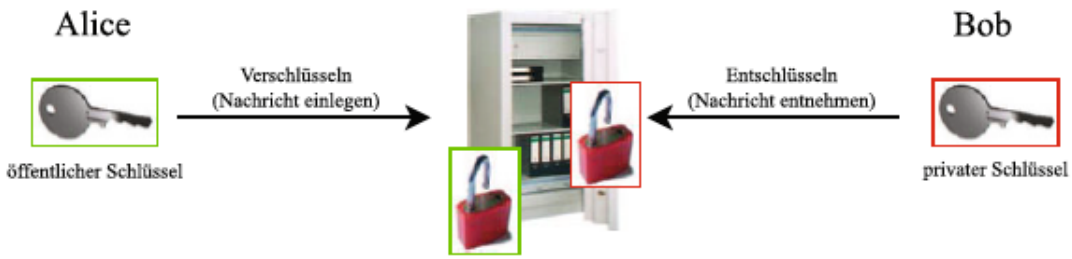

Abbildung 5. Analogie asymmetrischer Verschlüsselung[56]

Dieses Prinzip ist bei der asymmetrischen Kryptografie hingegen nicht notwendig. Hierbei muss der Schlüssel von Alice gar nicht geheim gehalten werden, wichtig ist, dass Bob als Empfänger mittels eines geheimen Schlüssels die Nachricht entschlüsseln kann. Dafür veröffentlicht Bob seinen Schlüssel zur Verschlüsselung und zusätzlich dazu noch einen privaten geheimen Schlüssel, den er für die Dechiffrierung der Nachricht benötigt. Somit besitzt Bob einen öffentlichen und einen privaten Schlüssel, die in der Literatur oft als private-key und public-key bezeichnet werden. Dieses Prinzip wird anhand eines Briefkastens gut veranschaulicht. Hier kann jeder einen Brief in den Briefkasten hineinwerfen, die Briefe rausholen und lesen, kann nur derjenige der den privaten Schlüssel für den Briefkasten hat. Dies hat den Vorteil, dass die Nachrichten, anders als bei der symmetrischen Verschlüsselung, nicht nur über einen sicheren Kanal ausgetauscht werden müssen.[57]

Das RSA-Kryptoverfahren (Rivest-Shamir-Adleman-Verfahren) ist das meistgenutzte asymmetrische Kryptoverfahren. Es wird verwendet, um kleine Datenmengen und digitale Signaturen zu verschlüsseln, wie z.B. Internetzertifikate. Das RSA-Verfahren besitzt jedoch einen sehr hohen Rechenaufwand und ist dementsprechend viel langsamer als das bereits beschriebene AES-Verfahren. Die Hauptfunktion von RSA ist daher der Schlüsseltransport für eine symmetrische Chiffre. In der Praxis wird RSA deshalb mit dem symmetrischen Algorithmus des AES verwendet.[58]

---

[56] Vgl. Paar, C./Pelzl, J. 2016, S. 176.

[57] Vgl. ebenda, S. 173 ff.

[58] Vgl. ebenda, S. 199 ff.

Das dritte und letzte Verfahren, welches in dieser Arbeit beschrieben wird, sind die kryptografischen Protokolle bzw. Hash-Funktionen. In den Hash-Funktionen wird ein Wert aus einer Nachricht berechnet, der als Fingerabdruck der Nachricht bewertet werden kann. Im Gegensatz zu den beiden vorgestellten Verfahren benötigt die Hash-Funktion keinerlei Schlüssel. Die Hash-Funktionen spielen eine wichtige Rolle bei digitalen Signaturen, denn anders als bei dem RSA-Verfahren, ist der Klartext der digitalen Signatur nicht in der Größe begrenzt.

In der Praxis enthalten oft E-Mails schon eine Größe von 128 bis 384 Byte, welche von dem RSA-Verfahren nicht verwirklicht werden kann, allerdings aber von den Hash-Funktionen. Ein Basisprotokoll für digitale Signaturen mit der Hash-Funktion könnte wie folgt aussehen:[59] Bob möchte eine digital signierte Nachricht an Alice senden, dafür berechnet Bob erst einmal den Hash-Wert der Nachricht x und signiert den Hash-Wert z mit seinem privaten Schlüssel. Alice möchte die Nachricht selbstverständlich lesen können, dafür berechnet sie den Hash-Wert z' der Nachricht x. Anschließend verifiziert sie die Signatur mit dem öffentlichen Schlüssel von Bob. Die Signaturerzeugung und die Verifikation haben in beiden Fällen den Hash-Wert z, deshalb wird der Hash-Wert in der Literatur auch Fingerabdruck der Nachricht genannt.[60]

3.2 Szenarioanalyse Cybercrime

Die Theorie, einen Cyberangriff oder Datenmissbrauch durchzuführen, konnten die beiden Sicherheitsexperten Charles Miller und Chris Valasek im Jahr 2015 anhand eines Jeep Cherokee erfolgreich auf die Praxis übertragen. In der Konferenz Black Hat USA erklärten sie den Erfolgsweg ihres Angriffes, welcher als Grundlage dieses Unterkapitels und der Anwendung der zuvor beschriebenen Cybersecurity- und kryptografischen Modellen bzw. Theorien dient.[61]

---

[59] Vgl. Ernst, H. et al. 2016, S. 440 ff. (online, URL siehe Literaturverzeichnis).

[60] Vgl. Paar, C./Pelzl, J. 2016, S. 335 ff.

[61] Vgl. Kaspersky 2020i (online, URL siehe Literaturverzeichnis).

Gestartet sind die beiden Experten mit dem Eindringen in den kostenpflichtigen WLAN Account des Herstellers Chrysler. Dieser unterliegt einer Verbindung zu dem Smartphone des Fahrers, welcher aktiv seine Daten teilt und somit eine Art WLAN-Hotspot entstehen lässt. Das Brechen eines WLAN-Schlüssels stellt heutzutage für erfahrene Hacker, zu denen letztendlich auch Miller und Valasek zählen, keine erwähnenswerte Hürde dar. Fahrzeuge von Chrysler generieren ihr WLAN-Passwort automatisch an dem Zeitpunkt, bei dem das Auto inklusive Multimediasystem zum ersten Mal in Betrieb genommen wird. Dies scheint zunächst in der Praxis eine sichere Methode zu sein, da die Kombination aus Datum und sekundengenauer Zeit etliche Millionen Schlüssel-Möglichkeiten ergibt.

Allerdings verringert sich die Anzahl der Alternativen erheblich, sobald das Fabrikationsjahr bekannt ist und der Monat richtig erraten wurde, hiernach verbleiben schließlich ca. 15 Millionen Kombinationen. Zusätzlich angenommen wird eine Produktion während der Tageszeit, welche die Anzahl der Eventualitäten bereits auf ca. 7 Millionen minimiert. Diese Anzahl ist für einen Hacker verhältnismäßig gering und allein durch das reine Ausprobieren der Codes, der sogenannten Brute Force Attacke, wird das gewünschte Ergebnis in kürzester Zeit erreicht.[62] Allerdings gibt es bei dieser Methode einen Nachteil: Um das WLAN-Passwort zu hacken, muss dem Jeep mindestens eine Stunde gefolgt werden, um eine konstante WLAN-Verbindung aufrecht zu erhalten.[63]

Miller und Valasek fanden hierfür jedoch einen schnelleren Weg: Beim erstmaligen Hochfahren des Systems erfasste dies die Zeit vom 01. Januar 2013 00:00 Uhr. Mit dem Wissen, dass eine bestimmte Zeit zur Verbindung mit dem GPS oder dem Mobilfunknetz benötigt wird, um genau zu sein 33 Sekunden, konnte das WLAN-Passwort gehackt werden. Dies war möglich, da Chrysler das WLAN-Passwort vor dem Einstellen der Zeit und des Datums generiert plus der Sekunden, in denen das Steuergerät hochfährt.[64] Diese Erkenntnis war der Durchbruch zum Infotainment-System, welches sie über den Hotspot erreichten.

---

[62] Vgl. Kaspersky ebenda.

[63] Vgl. Miller, D.C./Valasek, C., S. 18 ff.

[64] Vgl. Kaspersky 2020i (online, URL siehe Literaturverzeichnis).

Sie kontrollierten den Musik-Player und stellten das Radio in gewünschte Lautstärken ein, was bei hohen Geschwindigkeiten per Störgeräusche ziemlich gefährlich sein kann.[65]

Eine Handy-Basisstation, genannt Femtozelle, brachte die beiden Sicherheitsexperten auf eine weitere Möglichkeit den Jeep zu hacken. Eine Femtozelle erfüllt dieselben Zwecke wie ein Mobilfunkmast, der dem Nutzer einen verbesserten Empfang bieten soll. Durch die Femtozelle gelangten sie in das interne Netzwerk des Chryslers, also machten jeden einzelnen Jeep des Herstellers angreifbar. Problematisch hierbei war jedoch die Lokalisierung und die Übernahme eines individuell gewählten Fahrzeugs, statt der breiten Masse. Somit führten sie einen Massen-Scan durch um die IP-Adressen herauszufinden, die auf gewisse Anrufe reagierten und fanden somit heraus, welcher Chrysler mit dem gewünschten Bedienteil ausgestattet ist.[66]

Zusätzlich hackten die beiden Experten das GPS-Tracking-System (Global Positioning System) und konnten jeden gewünschten Jeep verfolgen und genauestens die Fahrtroute des Insassen auslesen. Unter der Hinzunahme dieser Information konnten sie nach Belieben auf die einzelnen Multimediasysteme bzw. Infotainment-Systeme zugreifen.[67] Dieser Fall lässt sich mit den Kryptografie-Protagonisten Bob und Alice anschaulich darstellen:

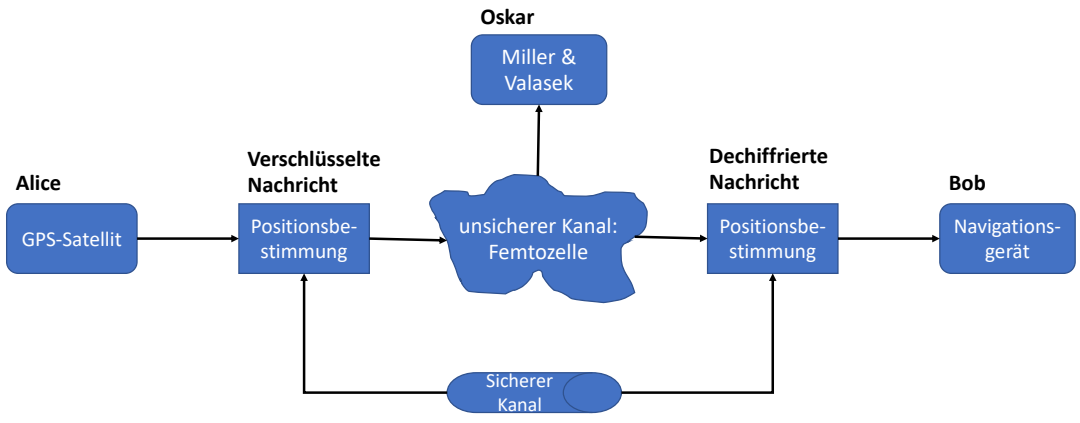

Abbildung 6. Symmetrische Verschlüsselung am Beispiel des GPS-Trackers - Eigene Darstellung

[65] Vgl. Miller, D.C./Valasek, C., S. 25.

[66] Vgl. Kaspersky 2020i (online, URL siehe Literaturverzeichnis).

[67] Vgl. Miller, D.C./Valasek, C., S. 44 ff.

Alice kann als GPS-Satellit angesehen werden, wobei Bob das dementsprechende Navigationsgerät darstellt. In der Angreiferrolle sind die beiden Sicherheitsexperten Miller und Valasek. Als Kommunikationskanal wird die Femtozelle bzw. das Mobilfunknetz definiert. Diese scheint auf dem ersten Blick für Chrysler als sicherer Kanal, allerdings zeigte Oskar auf, dass dieser als unsicher einzustufen ist.

Das Gespräch zwischen Alice und Bob soll geheim gehalten werden, da GPS-Daten zu den geheimen Komforts- und Sicherheitsfunktionsdaten zählen und somit von anderen Personen, die nicht zwingend mit den beiden kooperieren, verschlossen bleiben sollen. Der Ablauf ist wie folgt: Alice sendet ihre Positionsbestimmung über einen Satelliten an Bob. Die verschlüsselte Nachricht bzw. das Chiffrat gleitet dabei durch einen Kommunikationskanal, in diesem Fall durch den Mobilfunk. Bob besitzt denselben geheimen Schlüssel wie Alice und kann somit die Nachricht entschlüsseln. Somit kann Bob die Nachricht lesen und die Positionsbestimmung via GPS-Tracking ist abgeschlossen. Alice und Bob scheinen sich der Sache sicher zu sein und rechnen in dem gesamten Konstrukt nicht mit Oskar. Oskar verschafft sich jedoch unbemerkten Zugriff auf den Kanal durch das Hacken des Mobilfunknetzes mittels der Femtozelle. Dadurch hat Oskar uneingeschränkten Zugriff auf die Konversation zwischen Alice und Bob und kann diese mitlesen. Durch diese Methode gelang es Miller und Valasek den gewünschten Jeep virtuell zu verfolgen, ohne diesen, wie im vorigen Versuch, eine Stunde lang hinterherfahren zu müssen.

Um noch mehr Kontrolle über das Fahrzeug zu gelangen, galt es über das Infotainment- bzw. Multimediasystem hinaus den CAN-Bus zu hacken. Zwischen diesen beiden Kommunikationssystemen besteht jedoch keine direkte Verbindung, sodass diese Lücke über ein weiteres Netzwerk geschlossen werden musste.[68] Durch diese Problematik wurden sie auf den V850-Chip aufmerksam, denn das Infotainment-System kommuniziert mit diesem und der V850-Chip wiederum mit dem CAN-Bus.[69] Der V850-Chip wurde mittels einer neu aufgespielten Firmware gehackt.

[68] Vgl. ebenda, S. 33.

[69] Vgl. Kaspersky 2020i (online, URL siehe Literaturverzeichnis).

Dies gelang durch die falsche Übertragung von Daten über das Infotainment-System, welches ein Zugriff auf das Bussystem des Jeeps ermöglichte.[70] Der erfolgreiche Angriff auf das Bussystem brachte Miller und Valasek schlussendlich an das Ziel, woran sie seit über einem Jahr gearbeitet haben: Die vollständige Übernahme eines Automobils. Auch dieser Fall wird anhand von Alice und Bob näher veranschaulicht:

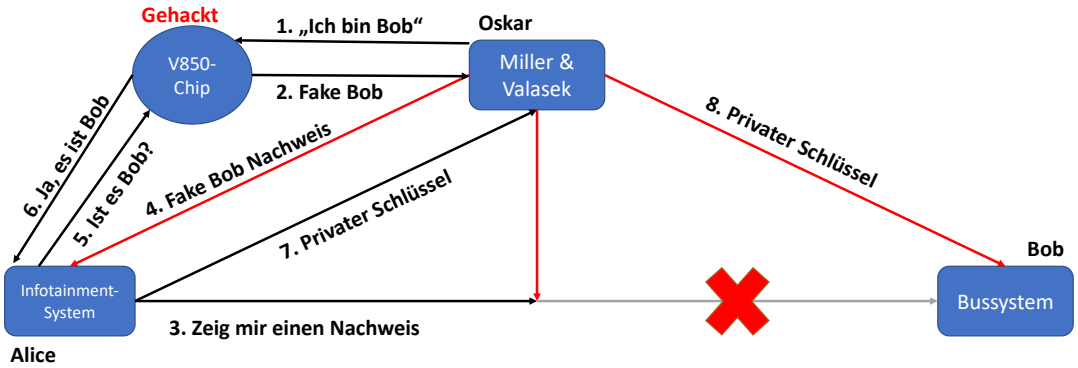

Abbildung 7. Asymmetrische Verschlüsselung am Beispiel des Bussystems - Eigene Darstellung

In diesem Verfahren ist Alice das Infotainment-System, womit sich Miller und Valasek (Oskar) den Zugriff auf das Bussystem (Bob) ermöglicht haben. Oskar bestimmt die Datenaussendung des V850-Chips, indem er sich als Bob ausgibt. Nach der Zusendung aller Daten des “Fake Bobs”, versucht Oskar einen direkten Zugriff auf das Bussystem zu generieren. Dies geht allerdings nicht, da Alice die Rolle des Türstehers darstellt. Alice fragt den echten Bob nach einem Nachweis, dass dieser wirklich Bob ist, jedoch blockt Oskar diese Nachricht ab und schaltet sich dazwischen. Dieses Phänomen wird in der Literatur als Man-In-The-Middle-Attack bezeichnet. Nach der Aufforderung von Alice, eine Bestätigung von Bob zu bekommen, sendet Oskar seinen “Fake Bob” Beleg. Alice überprüft diesen Nachweis mittels Rücksprache mit dem V850-Chip. Dieser wird im Normalfall eine negative Antwort zurückmelden, aber da Oskar den V850-Chip gehackt hat, antwortet dieser mit einer positiven Antwort und Alice geht davon aus, dass sie an Bob berichtet. Dementsprechend ist Bob ebenfalls der Überzeugung, dass er mit Alice kommuniziert, da der V850-Chip dieselben Hashwerte an Alice sendet.

[70] Vgl. Miller, D.C./Valasek, C., S. 48 ff.

Somit kann er fälschlicherweise sicher sein, dass Alice die Nachricht auch signiert hat. Wäre hier eine Abweichung des Hashwertes zu erkennen, würde Bob stutzig werden und erfahren, dass die Nachricht nicht von Alice signiert wurde. Mit dem ihr bekannten Wissen, übermittelt Alice den privaten Schlüssel an Oskar. Mit diesem inoffiziellen Schlüssel hat Oskar nun Zugriff auf das Bussystem und dementsprechend, wie weiter oben beschrieben, die vollständige Kontrolle über den Jeep.

Folglich wird an dem beschriebenen Szenario ergänzend zur Kryptanalyse das Scheitern des Cybersecurity Engineering anhand der TARA-Analyse inklusive der Bedrohungsidentifikation und der Risikobewertung durchgeführt. Mittels der strukturierten STRIDE-Analyse können die eingetretenen Bedrohungen übersichtlich und vollständig erfasst werden. Zur Eingliederung in das in Kapitel 3.1.2 beschriebene STRIDE Modell, werden in der folgenden Abbildung die STRIDE-Bedrohungen mit den tatsächlich vorliegenden Szenario-Bedrohungen abgeglichen und das Scheitern verschiedener Security-Ziele symbolisiert und anschließend erläutert.

Tabelle 1. STRIDE Bedrohungen des Jeep Cherokees - Eigene Darstellung

STRIDE Bedrohung	***Erklärung***	***Security-Attribut***	***Betroffenes System im Jeep Cherokee***
Spoofing	Vortäuschung einer falschen Identität	Authentifizierung	Web-Server
Tampering	Manipulation von Daten	Integrität	V850-Controller
Repudiation	Leugnung vom Angriff	Unleugbarkeit des Ursprungs	Nicht betroffen
Information Disclosure	Angreifer sieht geheime Daten	Vertraulichkeit	GPS-Tracking
Denial of Service	Störung der Verfügbarkeit der Anwendung	Verfügbarkeit	Radio
Elevation of Privilige	Angreifer erhöht eigene Berechtigung	Autorisierung	Eigene Firmware

Miller und Valasek konnten laut der erstellten Tabelle fünf von sechs STRIDE-Bedrohungen erfolgreich durchführen und die Attribute Authentifizierung, Integrität, Vertraulichkeit, Verfügbarkeit und Autorisierung brechen.

Durch das Täuschen des Web-Servers integrierten sie sich als neue Person in das vorhandene System. Anhand Alice, Bob und Oskar wurde bereits das Beispiel der Manipulation von Daten und somit der Bedrohung des Tamperings erklärt. Den Angriff auf die Steuergeräte hielten die beiden Sachkenner keineswegs geheim, vielmehr zeichnete sich die Übernahme durch das Einstellen des Radios oder der Scheibenwischer deutlich ab.

Durch das Umgehen der symmetrischen Verschlüsselung, indem wirksam Daten des GPS-Senders abgefangen wurden, zeigte das weitere Beispiel von Alice, Bob und Oskar auf, wie auch die Vertraulichkeit des Systems außer Gefecht gesetzt wurde. DoS-Angriffe (Denial of Service) wurden in Form des Radios veranschaulicht, auf das der Insasse keinen eigenständigen Zugriff mehr hegte. Beim Elevation of Privilege geht es um die Schaffung von erweiterten Zugriffsrechten, auch Administratorenrechte genannt. Wie es in der Computerwelt üblich ist, hat eine Person mit Administratorenrechten vollen Zugriff auf das System. Dies wurde bei dem Angriff durch die vollständige Übernahme des Jeeps erreicht und daher war das Schutzziel der Autorisierung unerfüllt.

Um das beschriebene STRIDE-Modell anzuwenden, wird in Abbildung 8 die Abfolge der Bedrohungstypen und das jeweilige Scheitern des Sicherheits-Attributs in Form eines Attack Trees angewandt.

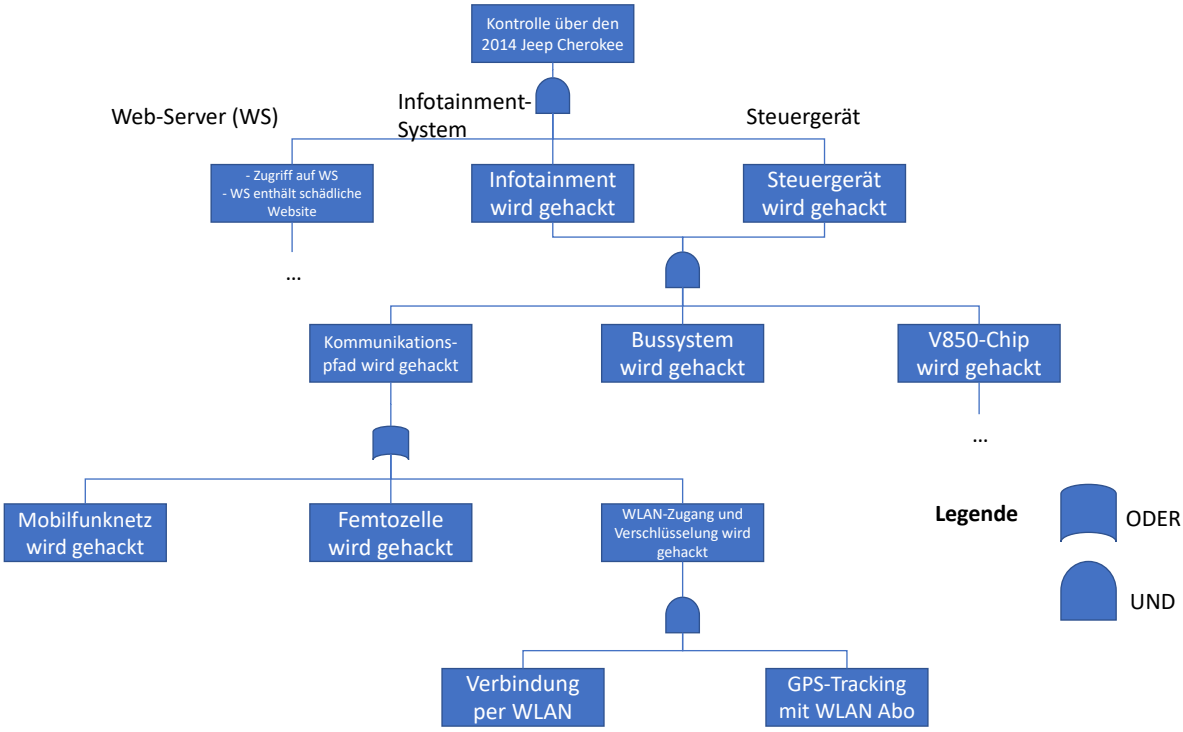

Abbildung 8. Attack Tree des Jeep Cherokees - Eigene Darstellung

An der Wurzel steht hier das Angriffsziel “Kontrolle über den 2014 Jeep Cherokee”. Als Zwischenziel, der sogenannte Vaterknoten, ist das Infotainment-System, das Steuergerät und der Web-Server definiert und mit einem logischen UND verknüpft. Die Kinder der zwei Vaterknoten Infotainment-System und Steuergerät bilden der Kommunikationspfad, das Bussystem und der V850-Chip. Mobilfunknetz, Femtozelle und der WLAN-Zugang bzw. WLAN-Verschlüsselung sind die Knotenkinder des Kommunikationspfades. Diese sind mit einem logischen ODER miteinander verknüpft. Den Abschluss bilden schließlich die Verbindung per WLAN und das GPS-Tracking mit dem WLAN-Abonnement, zugehörig zu dem WLAN-Zugang bzw. der Verschlüsselung als Vater.

Mit der STRIDE-Analyse und der Übertragung der Bedrohungsarten auf den gezeigten Angriffsbaum gilt die Bedrohungsidentifikation als abgeschlossen. Um das Gesamtbild der TARA zu vervollständigen müssen nachfolgend die Maßnahmen der Risikobewertung getroffen werden.

Dies erfolgt anhand des in Kapitel 3.2.1 beschriebenen HEAVENS-Modells und umfasst die Wahrscheinlichkeit sowie den Schweregrad des Jeep-Szenarios mittels einer 5-stufigen Skala. Dabei erfolgt die Ergebnisdarstellung anhand der dargestellten Risikomatrix in Abbildung 9.

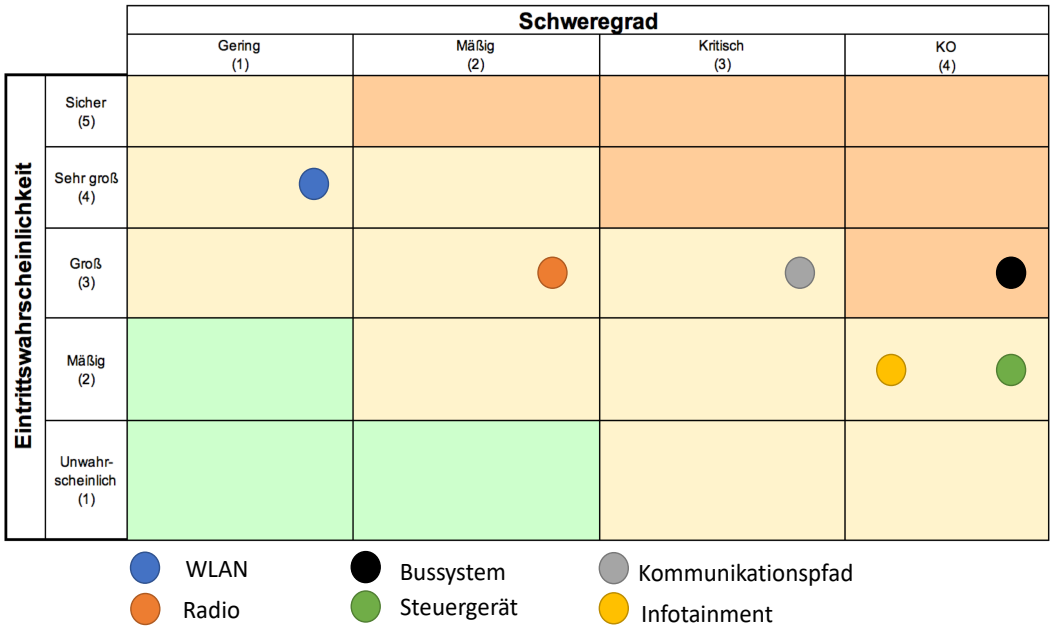

Abbildung 9. Risikomatrix der Fahrzeugsystemen des Jeep Cherokees - Eigene Darstellung

Komplementär stehen sich die beiden Begriffe WLAN (blau) und Steuergerät (grün) in der Matrix gegenüber. Seitens der Wahrscheinlichkeitsbestimmung lässt sich die Differenz sowohl über den Zugriffstypen, als auch die Kenntnisse und Fähigkeiten erklären. Der Hack eines WLAN-Netzes ist nicht nur in der Automobilwelt ein bekanntes Thema, sondern erhält die Breite der Community durch die allgemeine PC-Welt. So ist hier, im Gegensatz zum Steuergerät, breit gefächertes Fach- und Systemwissen, als auch die benötigte Ausrüstung gegeben.

Gesteigert wird die Eintrittswahrscheinlichkeit entlang der y-Achse durch den Zugriff auf ein logisches System, welches auf direktem Weg erreicht werden kann. Das physische Ziel, die Übernahme eines Steuergeräts, kann nur über mehrere Umwege erzielt werden. So bilden das WLAN-Netzwerk und die Steuergeräte den maximalen bzw. minimalen Rahmen der Eintrittswahrscheinlichkeit, unter dem die weiteren Parameter logisch zugeteilt worden sind.

Auch bezüglich der x-Achse, welche den zugeführten Schaden durch die Übernahme des jeweiligen Systems beschreibt, steht das WLAN gegenüber dem Steuergerät im Kontrast. So ist nach dem HEAVENS-Modell bei einem Angriff auf das WLAN-Netz mit dem Scheitern des Verlusts der Vertraulichkeit nur eine der vier Kategorien betroffen. Im Gegensatz dazu ist die Übernahme der gesamten Steuergeräte der schwerwiegendste Fall des Schadensausmaßes und beeinflusst auch die finanzielle Auswirkung, Komfort- und Verfügbarkeitseinschränkung und Sicherheitsrelevanz.

Analog zur Eintrittswahrscheinlichkeit liegen die weiteren Systeme zwischen den beiden beschriebenen Extremen. So wird bei einem Angriff auf das Infotainment-System der Komfort bzw. die Verfügbarkeit deutlich eingeschränkt. Auch können durch die Übernahme des Infotainment-Systems beispielsweise GPS-Daten ausgelesen werden, die mit einer Heimatadresse bestückt sind und somit ein erheblicher Verlust von Vertrauen bzgl. der Garantie der funktionalen Sicherheit des OEMs stattfindet.

Die folgende Tabelle 2 fasst die Bewertungen des Schweregrads und der Eintrittswahrscheinlichkeit zusammen und ermittelt das Endergebnis des Schadensausmaßes.

Tabelle 2. Schadensausmaß der Angriffe auf die Fahrzeugsysteme - Eigene Darstellung

Name	***Schweregrad***	***Eintrittswahrschein-lichkeit***	***Schadens-ausmaß***
WLAN	1	4	**Mittel**
Radio	2	3	**Mittel**
Bussysteme	4	3	**Hoch**
Kommunikationspfade	3	3	**Mittel**
Infotainment-System	4	2	**Mittel**
Steuergerät	4	2	**Mittel**

3.3 Weitere Angriffsmöglichkeiten

Das Anwendungsbeispiel von Miller und Valasek ist nur ein Bruchteil von dem, was einem Connected Car an Angriffsgefahren droht. Mit dem Zugriff auf das CAN-Bussystem und den jeweiligen Steuergeräten hat ein Angreifer die Kontrolle über das gesamte Fahrzeug. Dies hat verheerende Auswirkungen auf die Sicherheit und kann ggf. sogar tödliche Folgen haben. Eingeteilt werden die weiteren Angriffe in zwei Kategorien, zum einen in die funktionalen Cybersecurity-Angriffe und zum anderen in den Datenmissbrauch.

Beim funktionalen Angriff wird die Funktionalität der Steuergeräte beeinflusst und stellt somit eine Personenbedrohung dar. Funktionale Angriffe die fahrsicherheitsrelevant sind, sind z.B.: Bremssysteme, Tempomat, allgemeine Lenkung und Scheibenwischer. Zu den nicht fahrsicherheitsrelevanten funktionalen Angriffen gehören: Heizung, Belüftung, Navigationssysteme, elektrische Fensterheber und Multimediasysteme.

Der Datenmissbrauchsangriff ist in der Regel genauso fahrsicherheitsirrelevant, er zielt vielmehr auf die betrügerische Absicht ab. Zum Datenmissbrauch zählen Bedrohungen wie z.B.: Identitätsdiebstahl, Missbrauch von Datenverbindungen durch Dritte und das Einspielen von falscher Firmware, die bedrohlich hinsichtlich der C2C-Kommunikation sein können.

Diese Kategorie von Attacken können auf verschiedenster Art und Weisen stattfinden. Bei dem Angriff auf den Jeep wurden bereits einige verdeutlicht, weitere wären z.B.: das Einspielen von unerwünschten Apps oder auch eine Art Cyber-Erpressung, wobei nur bei der Bezahlung von Lösegeld das Fahrzeug wieder freigegeben wird. Das Connected Car besitzt hierbei viel Fläche für Übergriffe und durch die Vernetzung entstehen noch mehr Zugangskanäle als üblich. Angriffe können z.B. über WLAN, WLAN-Hotspot, Mobilfunknetz, Bluetooth und Apps stattfinden.[71]

[71] Vgl. Johanning, V./Mildner, R. 2015, S. 89 ff.

4. Diskussion

Die Kernabsicht hinter der Diskussion ist das Aufgreifen der Forschungsfrage aus der Einleitung, wonach zu erörtern ist, ob dem Nutzer vernetzter Fahrzeuge ein gewisser Cybersecurity-Standard gegeben werden kann und welche Maßnahmen getroffen werden müssen, um diesen zu erhöhen.

Klare Stärken liegen in der Bedeutungszusprechung des Themas Sicherheit in der Gesellschaft. Nicht nur der OEM setzt sich das erstrebenswerte Ziel, auch mit der Absicht der Steigerung von Absatzzahlen, die Car IT sicherer zu gestalten, sondern werden mit Standards wie unter anderem der Norm 26262 und klarer Richtlinien staatlicherseits unterstützt. Die Hinzunahme der gesamten Lieferantenkette, welche unter der Auflage ordert, mindestens die zweite Stufe des Automotive SPICE Standards erreicht zu haben, wird jeder Teilnehmer in die maximale Beisteuerung von Car-IT-Sicherheit einbezogen und der Produktlebenszyklus des Automobils vervollständigt.[72]

Jedoch wurden bereits in dieser Thesis anhand eines einzelnen Szenarios etliche Sicherheitsvorkehrungen gebrochen und widerlegt. So ist zudem ein Negativ-Bericht dieser Art keine Seltenheit, sondern wird vielmehr anhand zahlreicher Skandale in der Medienwelt belegt. So ist der Hackerangriff von Miller und Valasek längst kein Einzelfall, sondern vielmehr ein Sonderfall geworden. Die beiden Experten zählen mit ihrem Erfolg, ein explizit ausgewähltes Fahrzeug zu hacken, zwar zur Königsklasse, jedoch gehört die Infiltration von Massen-Steuergeräten bereits zu einem Standard-Hackertool in der Automobilindustrie.[73]

Die aktive Zusammenarbeit mit erfahrenen IT-Angreifern zeigt konträr neue Chancen für die Zukunft auf, um bestimmte Sicherheitslücken im Nachhinein zu korrigieren. So endet das Cybersecurity-Engeering nicht mit den beschriebenen Standards, sondern wird in Form von modernen Over-the-Air-Updates (kurz OTA) weiterentwickelt.[74]

---

[72] Vgl. ebenda, S. 93.

[73] Vgl. ebenda, S. 90 f.

[74] Vgl. Von Stokar, R. 2016, S. 21 ff.

Mittels dieser Lösung lassen sich, ohne des Aufsuchens einer Werkstatt, Sicherheitsupdates für den Schutz neuartiger Cyberattacken aufspielen. So kann dem, neben den Angreifern, meist gefährdeten Spieler entgegengewirkt werden: der Zeit. Auch fehlerhaft eingebaute Hard- und Software-Fehlern kann somit entgegengesteuert werden.[75]

Außerdem ist die zu anfangs angesprochene Vision Zero ein enormer Motivator, den Blick auf die Cybersecurity und den Datenschutz zu legen. Gelingt eine Vereinheitlichung des magischen Dreiecks, besteht die Möglichkeit die Unfallraten auf den Straßen zu senken und das gesamte Straßennetz sicherer und effizienter zu gestalten.

Jedoch stehen diesen Hoffnungsträgern sicherheitsrelevante Risiken gegenüber: So endet die Problemlösung in einem Teufelskreis. Hacker sind in der Lage immer wieder neue Schwachpunkte im Automobil zu finden, bei denen nur eine nachträgliche Korrektur denkbar ist oder zu spät veranlasst wird. So wird kontinuierlich, ähnlich dem Fall Miller und Valasek, ständig das schwächste Glied in der Kette herausgefiltert und der Angriff auf die weiteren Systeme übertragen. Das Beispiel anhand Chryslers zeigte bereits alternative Folgen, die sich in dem Kreislauf zuspitzen. So steht der Hersteller vor einem enormen Kostenaufwand bzw. Umsatzverlust, sobald das Vertrauen der Kunden verloren geht. Die Entwicklungskosten steigen dem ungeachtet zeitgleich um bis zu 30-50% und können schließlich nicht mehr bewerkstelligt werden. Diese werden jedoch benötigt, um das Sicherheitspotenzial zu steigern: der OEM befindet sich in einer Abwärtsspirale.

Ein weiterer wichtiger Punkt ist die Steigerung des möglichen Angriffspotenzials durch die zunehmende Vernetzung und Ergänzung von Fahrzeugsystemen. Hier scheitern, ohne einer sprunghaften neuen Entwicklungsstufe, die aktuellen Rechenleistungen der Fahrzeuge, um den benötigten Sicherheitsanforderungen auch in Zukunft gerecht zu bleiben.[76] Auch den oben erwähnten OTA-Updates sind hier Grenzen gesetzt.

---

[75] Vgl. Isermann, R.(hrsg) 2018, S. 15 ff.

[76] Vgl. Cybersecurity Roadmap 2020d (online, URL siehe Literaturverzeichnis).

Zunächst lassen sich diese aktuell nur beschränkt auf “nicht-kritischen” Systemen, wie die des Infotainment-Systems aufspielen.[77] Zum anderen werden dieser eine sichere Datenverschlüsselung sowie Unmengen an Speicherkapazität zugeschrieben.[78]

Die Computerwelt dient als klarer Pionier im Themenbereich der IT-Sicherheit, welcher im Vergleich zur Autowelt standhafte Zahlen vorweisen kann. Hier liegen, im gleichen Jahr wie dem des Hackerangriffes auf den Jeep Cherokee, bereits 220 Millionen bekannte Schadsoftwaretypen vor, wobei sich die Möglichkeiten bei dem Hack eines PCs oder Smartphones auf den Datenmissbrauch begrenzen. Mit diesem Hintergrundwissen scheint die Erkenntnis, dass es eine völlige Fahrzeug-Cybersecurity nie geben wird, immer weiter in den Vordergrund zu rücken.[79] In Anbetracht des aktuellen Entwicklungsstandes kann diese These nicht falsifiziert werden, da genügend Beispiele in der Praxis das Gegenteil aufzeigen. So definieren enorme Sicherheitslücken, auch noch in den Standards existierend, und den einzelnen Härtefällen die Vernetzung des Fahrzeugs als unsicher und dem Insassen kann keine vollkommene Sicherheit gewährleistet werden.

5. Fazit

5.1 Zusammenfassung

Die Studienarbeit mit dem Thema “Gestaltung von Cybersecurity im vernetzten Automobil” betrachtet die internen und externen vernetzten Fahrzeugsysteme im Hinblick auf die derzeitige Sicherheit vertieft im Aspekt der Cybersecurity und legt heutige Standards und Sicherheitsverfahren dar.

Nach der Einführung in das Thema und der Vorstellung der zu thematisierenden Forschungsfrage erfolgt die Schaffung einer Wissensgrundlage, die zum Verständnis der Thesis notwendig ist. So wird der Begriff des Fahrzeugs vom vernetzten Fahrzeug abgegrenzt und die IT-Architektur sowie die relevanten Kommunikationssysteme näher beschrieben.

---

[77] Vgl. Entwicklung Interieur (online, URL siehe Literaturverzeichnis).

[78] Vgl. Schleicher, M. 2020.

[79] Vgl. Johanning, V./Mildner, R. 2015, S. 90.

Anschließend werden die drei Begriffe funktionale Sicherheit, Cybersecurity und Datenschutz miteinander in Beziehung gestellt. Es wird analysiert, welche Maßnahmen und Standards bereits in der Automobilindustrie existieren und was in dem Bereich des Engineerings beachtet werden muss. So stellen die Prinzipien Automotive SPICE, TARA mit STRIDE und HEAVENS, die symmetrische Verschlüsselung, die asymmetrische Verschlüsselung und die Hash-Funktionen mit ihren digitalen Signaturen einen Überblick des derzeitigen Entwicklungsstands dar.

Basierend auf diesen Grundlagen wird folgend die Theorie auf ein Szenario aus der Praxis übertragen. Dabei stellt die Repräsentativität des Hackerangriffes auf den Jeep Cherokee eine vorteilige Rolle dar. Somit können mehrere Angriffsmöglichkeiten angewandt werden.

Mit den Erkenntnissen aus der Szenarioanalyse werden zuletzt in Form einer SWOT-Analyse die Stärken und Schwächen sowie die Chancen und Risiken der Cybersecurity in der Automobilwelt gegenübergestellt. Entwicklungspotenziale stecken besonders in den Bereichen der Ausweitung weiterer Standards, der neuen Art von Over-the-Air-Updates und der allgemeinen Fokussierung auf das Thema Sicherheit in der Gesellschaft.

5.2 Ausblick

Die Fahrzeugwelt befindet sich im anfänglichen Eingliederungsstatus des Megatrends der Digitalisierung. Viele Systeme, Anforderungen oder Rahmenbedingungen, welche in anderen Bereichen der Digitalen Welt bereits verankert sind, müssen schrittweise auf die Automobilbranche übertragen werden. Den Aspekt der Cybersecurity und des Datenschutzes in der Phase des Fahrzeugdesigns zu berücksichtigen ist ein erster richtiger Schritt, jedoch müssen diese parallel zum Zyklus des Machine Learnings weiter wachsen.

So reicht es nicht aus, lediglich den Compliance Prüfungen gerecht zu werden, sondern das Bestreben, der Hacker-Welt immer einen Schritt voraus zu sein, muss sich in dem Handeln der OEMs, aber auch der Zulieferern, widerspiegeln.

Und während die Automobilbranche dagegen ankämpfen muss, dass die Vernetzung des Fahrzeugs die Sicherheitsaspekte nicht überrollt, häuft sich eine wachsende Anzahl an ungeklärten und offenen Fragen, auf die es aktuell keine Antworten bzw. zeitliche Festlegungen gibt. So hebt das Thema der Automobilvernetzung unbekannte Risiken hervor, die bis hinzu neuartigen Terroranschlägen oder den Übergriff auf ganze Fahrzeugplattformen ausreichen. In langwierigen politischen Diskussionen wird versucht, sich auf Antworten bezüglich der Verantwortungsrolle im Fall des Datenmissbrauchs zu einigen. Hier stehen Fragen hinsichtlich der Strafübernahme bis hin zu weiteren Strafmaßnahmen gegenüber dem Straftäter offen. Auch eine neue, komplexere Gesetzgebung wird es für die Autoindustrie geben müssen, welche ebenfalls in langen Debatten ausdiskutiert wird. Zudem werden weitere Themen wie beispielsweise Ethik aufgeworfen, in der die klassische Oma-Kind-Unterscheidung im Falle eines steuerbaren Unfalls ebenfalls als ungeklärt gilt.[80]

Daher gibt es einen offensichtlichen Paradigmenwechsel, der über Jahrzehnte andauern wird und derzeit keine umfassenden Sicherheitsgarantien bieten kann. Die Vision Zero wird demnach zunächst eine Illusion bleiben, die es Stück für Stück zu realisieren gilt. So gestaltet sich die Selbststeuerung als sicherere Variante für die tägliche Straßennutzung und ist nicht mit dem Hobby-Reitpferd gleichzusetzen.

[80] Vgl. ebenda, S. 104 ff.

Literaturverzeichnis

Borgeest, K. (2008): Elektronik in der Fahrzeugtechnik: Hardware, Software, Systeme und Projektmanagement ; mit 25 Tabellen, 1. Aufl Wiesbaden: Vieweg.

Hansen, M. (2015): Das Netz im Auto & das Auto im Netz: Herausforderungen für eine datenschutzgerechte Gestaltung vernetzter Fahrzeuge In: *Datenschutz und Datensicherheit - DuD*, 39 (6): 367–371, DOI: 10.1007/s11623-015-0431-7.

Horváth, P./Seiter, M. (2012): Steuerung des Transformationsprozesses zum Lösungsanbieter - Entwicklung eines spezifischen Performance Measurement-Systems In: *Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung*, 64 (S65): 25–44, DOI: 10.1007/BF03373005.

Huber, E. (2015): Sicherheit in Cyber-Netzwerken: Computer Emergency Response Teams und ihre Kommunikation.

Isermann, R. (2018): Fahrerassistenzsysteme 2016: Von Der Assistenz Zum Automatisierten Fahren 2. Internationale ATZ-Fachtagung Wiesbaden: Springer Vieweg.

Islam, R./Refat, R.U.D. (2020): Improving CAN Bus Security by Assigning Dynamic Arbitration IDs In: *Journal of Transportation Security*, 13 (1–2): 19–31, DOI: 10.1007/s12198-020-00208-0.

Johanning, V./Mildner, R. (2015): Car IT kompakt: das Auto der Zukunft -- vernetzt und autonom fahren Wiesbaden: Springer Vieweg.

Krauß, C./Waidner, M. (2015): IT-Sicherheit und Datenschutz im vernetzten Fahrzeug: Bedrohungen und Herausforderungen In: *Datenschutz und Datensicherheit - DuD*, 39 (6): 383–387, DOI: 10.1007/s11623-015-0434-4.

Küsters, R./Wilke, T. (2011): Moderne Kryptographie: eine Einführung, 1. Aufl Wiesbaden: Vieweg + Teubner.

Paar, C./Pelzl, J. (2016): Kryptografie verständlich: ein Lehrbuch für Studierende und Anwender Berlin Heidelberg: Springer Vieweg.

Sänn, A./Richter, S./Fraunholz, C.K. (2017): Car-to-X als Basis organisationaler Transformation und neuer Mobilitätsleistungen In: *Wirtschaftsinformatik & Management*, 9 (5): 60–71, DOI: 10.1007/s35764-017-0107-1.

Schleicher, M. (2020): Absolute Sicherheit wird es beim automatisierten Fahren nie geben In: *ATZextra*, 25 (S1): 6–9, DOI: 10.1007/s35778-020-0114-3.

Schnieder, L./Hosse, R.S. (2018): Leitfaden Automotive Cybersecurity Engineering: Absicherung vernetzter Fahrzeuge auf dem Weg zum autonomen Fahren Wiesbaden: Springer Vieweg.

Spitz, S./Pramateftakis, M./Swoboda, J. (2011): Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen, 2., überarb. Aufl Wiesbaden: Vieweg + Teubner.

Von Stokar, R. (2016): Software Updates — Efficient Use of Connected Cars In: *Auto Tech Review*, 5 (1): 20–23, DOI: 10.1365/s40112-016-1085-z.

Zimmermann, W./Schmidgall, R. (2007): Bussysteme in der Fahrzeugtechnik: Protokolle und Standards ; mit 99 Tabellen, 2., aktualisierte und erw. Aufl Wiesbaden: Vieweg.

Internetquellen

CAN-Bussysteme IT Wissen (2020h): CAN (controller area network) :: CAN-Bus :: ITWissen.info. Online im Internet: https://www.itwissen.info/CAN-controller-area-network-CAN-Bus.html, Stand: 02.09.2020.

Cybersecurity Roadmap (2020d): 2018-DE-pdf-Cyber-Security-Roadmap-fuer-vernetzte-Fahrzeuge.pdf. Online im Internet: https://de.nttdata.com/-/media/NTTDataGermany/Files/2018-DE-pdf-Cyber-Security-Roadmap-fuer-vernetzte-Fahrzeuge.pdf, Stand: 30.08.2020.

Elektronik Kompendium (2020a): Car-to-Car-Kommunikation (C2C, Car2Car). Online im Internet: https://www.elektronik-kompendium.de/sites/kom/1509151.htm, Stand: 12.07.2020.

Elektroniknet (2020g): Online im Internet: https://www.elektroniknet.de/elektronik-automotive/assistenzsysteme/schutz-vor-neugierigen-zugriffen-16.html, Stand: 30.08.2020.

Elon Musk (2020c): Trump, Merkel, Röhrl, Clarkson: Zitate zum autonomen Fahren - auto motor und sport. Online im Internet: https://www.auto-motor-und-sport.de/verkehr/trump-merkel-roehrl-clarkson-zitate-zum-autonomen-fahren/, Stand: 30.08.2020.

Entwicklung Interieur (2020j): s35148-017-0075-z.pdf. Online im Internet: https://link.springer.com/content/pdf/10.1007/s35148-017-0075-z.pdf, Stand: 07.09.2020.

Ernst, H./Schmidt, J./Beneken, G. (2016): Grundkurs Informatik Wiesbaden: Springer Fachmedien Wiesbaden. Online im Internet: http://link.springer.com/10.1007/978-3-658-14634-4, Stand: 07.09.2020, DOI: 10.1007/978-3-658-14634-4.

Ernst, H./Schmidt, J./Beneken, G. (2020): Grundkurs Informatik: Grundlagen und Konzepte für die erfolgreiche IT-Praxis – Eine umfassende, praxisorientierte Einführung Wiesbaden: Springer Fachmedien Wiesbaden. Online im Internet: http://link.springer.com/10.1007/978-3-658-30331-0, Stand: 07.09.2020, DOI: 10.1007/978-3-658-30331-0.

Frauenhofer (2020e): Kryptografie für das Auto der Zukunft. Online im Internet: https://www.sit.fraunhofer.de/de/presse/details/news-article/show/kryptografie-fuer-das-auto-der-zukunft/, Stand: 30.08.2020.

Genua (2020f): Kryptografie: Von Schlüsseln und anderen Geheimnissen. Online im Internet: https://www.genua.de/aktuelles/v/kryptografie-von-schluesseln-und-anderen-geheimnissen.html, Stand: 30.08.2020.

Graf, F. (2009): „Car 2 Car/Car 2 X“ Kommunikation: Kommunikation zwischen Fahrzeugen und deren Umgebung In: https://www.uni-koblenz-landau.de/de/koblenz/fb4/ist/AGZoebel/Lehre/ss09/Seminar09/graf Stand: 31.08.2020.

Holland, H. (2019): Dialogmarketing und Kundenbindung mit Connected Cars: Wie Automobilherstellern mit Daten und Vernetzung die optimale Customer Experience gelingt. Online im Internet: https://doi.org/10.1007/978-3-658-22929-0, Stand: 29.06.2020.

IT-Wissen (2020b): C2I (car to infrastructure): Car-to-Infrastructure : ITWissen.info. Online im Internet: https://www.itwissen.info/C2I-car-to-infrastructure-Car-to-Infrastructure.html, Stand: 12.07.2020.

Kaspersky (2020i): Black Hat USA 2015: So wurde der Jeep gehackt. Online im Internet: https://www.kaspersky.de/blog/blackhat-jeep-cherokee-hack-explained/5940/, Stand: 04.09.2020.

Meinel, C./Sack, H. (2014): Sicherheit und Vertrauen im Internet Wiesbaden: Springer Fachmedien Wiesbaden. Online im Internet: http://link.springer.com/10.1007/978-3-658-04834-1, Stand: 07.09.2020, DOI: 10.1007/978-3-658-04834-1.

Miller, D.C./Valasek, C. (2015): Remote Exploitation of an Unaltered Passenger Vehicle In: http://illmatics.com/Remote%20Car%20Hacking.pdf Stand: 31.08.2020.

Raith, N. (2019): Das vernetzte Automobil: Im Konflikt zwischen Datenschutz und Beweisführung. Online im Internet: https://doi.org/10.1007/978-3-658-26013-2, Stand: 29.06.2020.

Eidesstattliche Erklärung

Ich versichere, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quelle kenntlich gemacht.

Hamburg, den ……. Wiliam Mahyar

Erklärung – Einverständnis

Ich erkläre mich damit

- einverstanden,
- nicht einverstanden

dass ein Exemplar meiner Bachelor- (Master-) Thesis in die Bibliothek des Fachbereichs aufgenommen wird; Rechte Dritter werden dadurch nicht verletzt.

Hamburg, den ……. Wiliam Mahyar