Stefan Kubica, Hagen Ringshausen,
Jörg Reiff-Stephan, Marius Schlingelhof (Hrsg.)
2. Automobil Symposium Wildau:
Tagungsband Technische Hochschule Wildau 2017

Steven Michna
Carmeq GmbH
steven.michna@carmeq.com

Christian Gierds
Carmeq GmbH
gierds.christian@carmeq.com

Security als Basisbaustein der Digitalisierung

Zusammenfassung

Die Digitalisierung hält Einzug in allen Bereichen des täglichen Lebens. Auch im Automotive-Sektor entwickeln sich die Systeme weiter und unterstützen zunehmend den Fahrer, steuern selbstständig das Fahrzeug oder erhöhen den Komfort.
Diese Veränderungen in der Art der Nutzung des Automobils öffnen auch neue Wege für Manipulationen und Angriffe, sodass selbst bisher bewährte sowie als sicher geltende Funktionen neuen Risiken unterliegen.
Aufgabe der Automobilindustrie muss es in diesem Zusammenhang sein, die Risiken und Herausforderungen im Themengebiet Security zu erkennen und bereits im Rahmen der Entwicklung präventiv anzugehen.

1. Einführung

In den vergangenen Jahren gab es vermehrt Meldungen über Fahrzeugdiebstähle, bei denen die Ursache auf eine Manipulation der schlüssellosen Fahrzeugzugangsfunktion zurückzuführen war. Während zuvor noch physischer Zugang zum Fahrzeug notwendig gewesen ist, so sind nun aufgrund der veränderten Funktionsweise beim Fahrzeugzugang neue potentielle Angriffsmöglichkeiten entstanden. Diese Diebstähle zeigen, dass die Angreifer in der Lage sind, solche Schwachstellen gezielt zu identifizieren und für ihre Zwecke zu missbrauchen. Von solchen Vorfällen waren bisher verschiedenste Marken und Zugangssysteme betroffen.
Durch die Einführung neuer Technologien wie zum Beispiel eines Smartphones als Schlüsselersatz ergeben sich weitere Risiken. Aufgrund unterschiedlicher Ansätze bei der Umsetzung solcher Konzepte, ergeben sich für Angreifer verschiedene Einfallstore. So war es beispielsweise bei einigen BMW-Modellen möglich, dass Daten durch Unbefugte von außen abgefangen und zum Fahrzeugzugang genutzt werden konnten [Zeit15]. Besonders kritisch war hierbei, dass das kompromittierte Schlüsselmaterial für Angriffe auf weitere Fahrzeuge der gleichen Marke genutzt werden konnte, da diese die gleichen Schlüssel im Rahmen ihrer kryptografischen Verfahren nutzten [Holl15]. Entgegen des Vorgehens bei dem zuvor skizzierten Szenario gelang es Hackern bei einem Modell von Tesla durch ein Lockangebot eine bereits bekannte Schwachstelle des Betriebssystems Android auszunutzen, indem der Fahrzeughalter dazu gebracht wurde eine schädliche App zu installieren. Damit

doi: 10.15771/ASW_2017_4

konnten Angreifer vertrauliche Daten für den Fahrzeugzugang abgreifen, die ebenfalls zum Starten genutzt werden können [Bay15].

Diese Beispiele sollen einen Einblick liefern, wie vielschichtig das Thema Security im Automobilbereich bereits ist. Eine steigende Vernetzung sowie die Digitalisierung bringen Risiken mit sich und eröffnen neue Ziele und Wege. Da sich die Beispiele lediglich auf eine einzelne Funktion des Fahrzeugs beziehen, gilt es in diesem Zusammenhang zu hinterfragen, wie der aktuelle Trend in der Entwicklung das skizzierte Risikopotential beeinflusst.

Mit dem großen Ziel der Automobilindustrie des „autonomen Fahrens" wird sich die bereits schon enorme Komplexität der Systeme weiter erhöhen. So gibt es beispielsweise in einem heutigen Kraftfahrzeug ungefähr 80 Millionen Zeilen Softwarecode, um die aktuellen Funktionsumfänge zu gewährleisten. Bereits aus Sicht der Funktionalen Sicherheit ist dies sehr kritisch zu betrachten, da die Anzahl der Fehler mit der Anzahl der Programmzeilen steigt [JoMi15]. Die Schlussfolgerung, dass sich auch die Anzahl möglicher Schwachstellen erhöht, liegt dabei nahe. Bezüglich der Komplexität der Fahrzeugsysteme muss zudem berücksichtigt werden, dass wir uns auf der 6-Stufigen Skala der SAE, welche die Stufen der Automatisierung abbildet, erst auf Stufe 2 befinden [SAE16]. Eine entsprechende Steigerung der Komplexität sowie ein damit verbundenes erhöhtes Angriffsaufkommen sind daher zu erwarten.

Verschiedenste Gruppierungen weltweit beobachten und diskutieren diese Entwicklung. Der Senator des Bundesstaates Massachusetts fasst dabei im Rahmen einer eigenen Analyse den Stand in 8 Haupterkenntnissen alarmierenden zusammen [Mark15]. Auch der Bundesverband der Verbraucherzentrale in Deutschland fordert mittlerweile, dass Automobilhersteller gemeinsam mit der Politik für die IT-Sicherheit vernetzter Fahrzeuge sorgen müssen, und misst der Datensicherheit dabei eine lebenswichtige Bedeutung zu [VZBV16].

Wenn man bedenkt, welche Entwicklungsaufwände bereits im Kontext der funktionalen Sicherheit gefordert und erbracht werden, dann ist diese Betrachtungsweise durchaus nachvollziehbar. Sollte es einem Angreifer gelingen, Teile der Systeme zu manipulieren, könnte er ebenfalls Sicherheitsmaßnahmen umgehen. Damit wird die Security eine Grundvoraussetzung für die Safety.

Im Folgenden geben wir einen Überblick, wie sich die Angriffsmöglichkeiten und -ziele durch die Entwicklung neuer Funktionen im Rahmen der Digitalisierung verändern, welche Herausforderungen sich dadurch für Hersteller im Bereich Security ergeben und welche Strategien zur Bewältigung sinnvoll erscheinen.

2. Angriffsmöglichkeiten und -ziele

2.1 Entwicklung und Veränderung der Fahrzeugfunktionen – neue Angriffsmöglichkeiten

Wie eingangs beschrieben, ist es derzeit insbesondere das „Autonome Fahren", welches die Automobilindustrie antreibt. In diesem Kontext werden automatisiert bzw. autonom agierende Systeme entwickelt. Sie bedienen sich verschiedenster Daten des eigenen Fahrzeugs, von weiteren Verkehrsteilnehmern, der Infrastruktur oder aber auch aus der Cloud.

Im Zuge dieser Entwicklung kommt es ebenfalls zu einer Weiterentwicklung im Bereich des Infotainments: So soll für den Kunden zum Beispiel die Zeit im Fahrzeug angenehmer gestaltet werden, während sich das Fahrzeug automatisiert bewegt.

Neben diesen direkten Entwicklungstrends gibt es noch einige weitere Funktionen, die aufgrund von Wartungszwecken, Sicherheit oder neuen Geschäftsmodellen zwingend erforderlich werden. Hierbei handelt es sich beispielsweise um Möglichkeiten, Updates aus der Ferne einzuspielen oder Zusatzfunktionen freizuschalten.

Die nachfolgenden Punkte tragen dabei im Rahmen der Umsetzung dieser neuen Systeme dazu bei, dass Angreifer leichter auf das Fahrzeug zugreifen können:

- Verwendung der Mobilfunknetze zur Kommunikation
- Nutzung von Informationen von außerhalb des Fahrzeugs
- Erhöhte Anzahl an Schnittstellentechnologien (Bluetooth, W-LAN, TV)
- Integration des Smartphones in die Funktionsabläufe
- Verwendung von Cloudsystemen, die Funktionsanteile übernehmen
- Vorhaben dient es für die Verbindung der Java-Api von Apache Spark mit dem Programmierframework Eclipse. Durch die lizenzfreie Nutzbarkeit, den offenen Quellcode, die Platt-formunabhängigkeit und die Tatsache, dass Apache Maven Teil der Apache Software Foundation ist, gilt, ebenso

2.2 Das Fahrzeug als Ziel eines Angriffs

Auch die Motivation der Angreifer verschiebt sich mit den beschriebenen Entwicklungen. Während der klassische Angreifer aus einem kriminellen Antrieb heraus handelt und primär Fahrzeugdiebstahl, Schädigung oder Datenklau im Fokus steht, werden zunehmend andere Typen von Hackern relevant. Vermehrt wird zusätzlich im wissenschaftlichen Kontext oder privat als „Hobby“ versucht, Fahrzeuge fern zu steuern oder Schwachstellen aufzuzeigen, was negative Presse und Imageverlust für die entsprechenden Hersteller mit sich zieht. Darüber hinaus wird es durch freischaltbare Software auch für den Fahrzeughalter selbst interessant, durch Manipulation Funktionsumfänge widerrechtlich zu erlangen. Dabei ist die Rolle des Angreifers für Fahrzeughalter keinesfalls neu. Bereits die Möglichkeit zur Tachomanipulation oder Leistungssteigerung durch Chiptuning ließ in der Vergangenheit Manipulation zu Ungunsten der Automobilhersteller zu. Dies erklärt, warum gerade solche Systeme schon heute mit teilweise komplexen Mechanismen geschützt werden. Einige Bedingungen fördern zudem die Attraktivität der Angriffe auf Fahrzeuge. Diese werden nachfolgend benannt:

- Einmal gefundene (Software-) Sicherheitslücken, lassen sich auf ganze Fahrzeugflotten anwenden
- Backendsysteme als Schaltzentrale ergeben attraktive Ziele für Datendiebstahl
- Reputation in der Hackerszene erhöht sich bei aufgedeckten oder durchgeführten Hacks
- Fahrzeugdiebstahl ist durch Funkschnittstellen schneller und mit geringerer Sichtbarkeit möglich

3. Security-Herausforderungen

Die Kombination der größeren Angriffsmöglichkeiten und der ebenfalls steigenden Zahl der Angriffsziele führt

dazu, dass die Automobilhersteller den daraus resultierenden Bedrohungen entgegenwirken müssen. Um das Ziel eines sicheren Fahrzeugs zu erreichen, ergeben sich daher verschiedene Herausforderungen, die sich in übergeordnete Themengebiete zusammenfassen lassen, wie sie in Abbildung 1 dargestellt sind.

Abbildung 1: Dimensionen der Security im Rahmen des Autonomen Fahrens

Zentrale Themenfelder für den Hersteller selbst sind insbesondere das Management bzw. die Anpassung seiner Aktivitäten in der ENTWICKLUNG sowie eine verstärkte Präsenz und Aktivität im Bereich FELDBEOBACHTUNG. Dabei geht es vor allem um die Integration von Security in bestehende Abläufe über den gesamten Lebenszyklus. Das notwendige Know-How muss auf- und stetig ausgebaut werden, um ausreichende Schutzlösungen identifizieren und umsetzen zu können. Zudem wird es in Zukunft noch wichtiger werden, Vorkommnisse im Feld zu beobachten und Rückschlüsse für zukünftige Projekte zu ziehen. Dies beinhaltet auch, zeitnah Updates für bestehende Systeme zu liefern.

Für die STANDARDISIERUNG hält die Security herstellerübergreifende Aufgaben bereit. Zur Kommunikation zwischen Fahrzeugen verschiedener Hersteller oder zukünftig auch mit der Infrastruktur müssen Schutzkonzepte und technische Umsetzungen international vereinheitlicht werden. Auch die Frage nach einer verwaltenden Instanz für kryptografisches Schlüsselmaterial oder einem allgemein akzeptierten Vertrauensanker für alle Verkehrsteilnehmer stellt sich in diesem Kontext. Als zweite markenübergreifende Herausforderung schließt sich die Klärung von Fragen im Rahmen der POLITIK und GESELLSCHAFT an. In welchem Maße die IT-Sicherheit gesetzlich vorgeschrieben bzw. reguliert werden muss, ist zu diskutieren. Offen ist ebenfalls das Thema Haftung bei Schäden durch Angriffe. Die Gültigkeitsbereiche solcher Regularien sollten einerseits genau definiert sein, andererseits erhält die Berücksichtigung und Umsetzung dieser Vorgaben bei Fahrzeugen, die in mehr als einem Land vermarktet werden, besondere Relevanz. Zuletzt stellen auch der KUNDE sowie der MARKT ein wichtiges Element im Gesamtkomplex dar. Das Security-Bewusstsein und die Wahrnehmung in diesem Bereich geben dabei den Handlungsspielraum für Schutzkonzepte vor, deren Wirksamkeit nur bei entsprechender Usability greift. Konkurrenten, Hackeraktivitäten und Wissenschaft dienen als Orientierung für potentiell neue Geschäftsfelder und ermöglichen eine Einschätzung des Stands der Technik.

4. Empfehlungen für die Automobilhersteller

Trotz der Vielseitigkeit der Herausforderungen trägt der Automobilhersteller

im Rahmen der Entwicklung den größten Anteil für sichere Systeme, weshalb insbesondere für dieses Feld nachfolgend einige Empfehlungen gegeben werden.

Das Fachgebiet der IT Security beschäftigt sich bereits mit dem Umgang von Sicherheitsrisiken und bietet dabei eine Vielzahl von Vorgehensweisen und technischen Lösungen zum Schutz vor- bzw. zum Umgang mit diesen. Die Automobilindustrie muss diese Mechanismen nun auf höchstem Niveau verstehen und beherrschen lernen [Burk14]. Sie sind in die Entwicklung zu integrieren und über den gesamten Produktlebenszyklus zu berücksichtigen. Security muss mit höchster Priorität in einem ganzheitlichen Ansatz über alle Bereiche hinweg betrachtet werden [SeWo15].

Es geht darum, einen Entwicklungsprozess zu etablieren, bei dem Security in jeder Phase betrachtet wird. Dazu muss der Hersteller frühzeitig seine Systeme strukturiert auf Risiken analysieren und die identifizierten Punkte müssen bei Design und der Implementierung des Systems berücksichtigt werden. Hierbei können bekannte Prinzipien für die Architektur, kryptografische Verfahren oder auch Secure Coding aus der IT-Security erste Ansätze für Maßnahmen liefern. Das Vorgehen ist ein iterativer Prozess und bei vielen Aktivitäten kann man von den weitgehend etablierten Prozessen der Funktionalen Sicherheit lernen, wodurch ein Effizienzpotential aber auch Abstimmungsbedarf entsteht. Am Ende muss die Mitigation der Risiken durch Tests nachgewiesen werden.

Der Fokus der Hersteller im Produktlebenszyklus liegt bisher meist auf der Entwicklung. Da jedoch die Security ein sehr schnelllebiges Themengebiet ist und eine Beobachtung des Feldes sowie eine umgehende Beseitigung von auftretenden Schwachstellen eine Grundvoraussetzung sind, ergeben sich viele neue Aktivitäten in die Phase nach der Produktion. Dies erfordert einerseits, dass Mechanismen zur Feldbeobachtung und IT-Forensik bereits in der Entwicklung berücksichtigt werden, damit eine sinnvolle Analyse und Ursachensuche bei auftretenden Hacks zielführend durchgeführt werden können. Auf der anderen Seite müssen entsprechende Prozesse zur Feldbeobachtung sowie Updatemechanismen eingeplant und im Ernstfall zeitnah umgesetzt werden.

Eine Schlüsselposition in diesem Zusammenhang könnte der Überwachung der Kommunikationsströme innerhalb des Fahrzeugs und anderer Teilnehmer sowie Backendsysteme zukommen [SeWo15]. Hierzu werden bereits Entwicklungspartnerschaften geschlossen und Lösungen, wie zum Beispiel auf der diesjährigen CES, vorgestellt [Flör17].

5. Fazit

Die Automobilindustrie wird durch die zunehmende Digitalisierung vor enorme Herausforderungen gestellt. Security nimmt in diesem Umfeld eine wachsende Rolle ein. Hauptaufgabe wird es dabei sein, eine durchgängige Integration in die bestehenden Prozesse zu gewährleisten. Von der IT-Security können dabei prozessuale und technische Themen übernommen werden. Bei der Umsetzung werden die Hersteller zunächst Ihre eigenen Wege und Lösungen einschlagen, während sich Best-Practices im Automotive-Umfeld erst ergeben werden. Auch Politik und Standardisierung müssen ihren Beitrag dazu leisten, indem

sie die Rahmenbedingungen festlegen. Da sich die Angreiferseite ebenfalls sehr dynamisch verändert, muss versucht werden diese zu verstehen und kontinuierlich zu beobachten. Dies ist die Voraussetzung, um adäquate Schutzmechanismen zu entwickeln und schnell reagieren zu können.

6. Literaturverzeichnis

[Bay15]
Bay, Lukas: Tesla stehlen – leicht gemacht. 2015, http://app.wiwo.de/unternehmen/industrie/hacker-kriminalitaet-tesla-stehlen-leicht-gemacht/14889720.html. Abruf am 10.01.2017.

[Burk14]
Burkert, Andreas: Fahrzeugvernetzung: Strategien gegen den Digitalen Crash. In: ATZ - Automobiltechnische Zeitschrift, Nr. 01 (2014), S. 28-33.

[Flör17]
Flörecke, Klaus-Dieter: Kooperation zum besseren Schutz autonomer Fahrzeuge. 2017, http://www.automobilwoche.de/article/20170104/NACHRICHTEN/170109968/1334/ces-2017-kooperation-zum-besseren-schutz-autonomer-fahrzeuge. Abruf am 10.01.2017.

[Holl15]
Holland, Martin: ConnectedDrive - Der BMW-Hack im Detail. 2015, https://www.heise.de/newsticker/meldung/ConnectedDrive-Der-BMW-Hack-im-Detail-2540786.html. Abruf am 16.01.2017.

[JoMi15]
Johanning, Volker; Mildner, Roman: Car IT kompakt: Das Auto der Zukunft – Vernetzt und autonom fahren. Springer, Wiesbaden, 2015.

[Mark15]
Markey, Edward: Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk. 2015, http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf. Abruf am 10.01.2017.

[SAE16]
SAE International: SAE J 3016 „Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems". 2016.

[SeWo15] Serio, Giuseppe; Wollschläger, Dirk: Cyber Security. In: ATZ - Automobiltechnische Zeitschrift, Nr. 06 (2015), S. 60-63.

[VZBV16]
Verbraucherzentrale Bundesverband e.V.: (Rechts-)sicher Fahren mit Autopilot: Positionen des vzbv zum automatisierten und vernetzten Fahren. 2017, http://www.vzbv.de/sites/default/files/16-12-05_positionspapier_vzbv_automatisiertes_und_vernetztes_fahren.pdf. Abruf am 10.01.2017.

[Zeit15]
ZEIT: Hacker konnten BMW-Türen jahrelang per Handy öffnen. 2015, http://www.zeit.de/mobilitaet/2015-01/bmw-hacker-sicherheit. Abruf am 10.01.2017.