Selbstdatenschutz im vernetzten Fahrzeug

Angreifermodell für Selbstdatenschutz im vernetzten Fahrzeug

Veröffentlichung Nummer: D1.5

Version 1.0

GEFÖRDERT VOM

Projekt Akronym: SeDaFa
Vollständiger Projekttitel: Selbstdatenschutz im vernetzten Fahrzeug
Projektwebseite: http://www.sedafa-projekt.de/

Veröffentlichungsdatum	02.08.2017
Seitenanzahl:	18
Schlagwörter:	Vernetztes Fahrzeug, Privatsphäre, Datenschutz, Selbstdatenschutz, Angreifermodell

Autoren:	Nadine Sinner	accessec GmbH
	Daniel Zelle	Fraunhofer SIT
	Rasmus Robrahn	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhaltsverzeichnis

1 Einleitung

IT ist einer der größten Innovationsmotoren in der Automobilindustrie und ist unabdingbar für viele Anwendungen wie z.B. Assistenzsysteme, Mehrwertdienste oder auch das autonome Fahren. Viele der dabei anfallenden Daten sind jedoch personenbezogen oder personenbeziehbar und ermöglichen z.B. die Erstellung von Bewegungsprofilen oder von Profilen des Fahrverhaltens des Fahrzeugnutzers. Ziel von SeDaFa ist es, neue Wege für den Selbstdatenschutz durch Fahrzeugnutzer zu entwickeln und bewerten.

Hierzu werden in SeDaFa neue Ansätze und Werkzeuge entwickelt, um Fahrzeugnutzern transparent darzustellen, welche Daten im Fahrzeug vorhanden sind, wie der Personenbezug aussieht, wie sie verarbeitet und weitergeleitet werden und welche Risiken bestehen. Weiterhin werden neue Ansätze entwickelt, die dem Fahrzeugnutzer eine selbstbestimmte Kontrolle bei der Weitergabe der eigenen Fahrzeugdaten ermöglicht.

In diesem Dokument wird ein Angreifermodell entwickelt, auf dessen Basis die in SeDaFa entwickelten Werkzeuge zum Schutz der im vernetzten Fahrzeug anfallenden Daten erarbeitet werden. Das Dokument dient damit zusammen mit dem Dokument „Anforderungsanalyse für Selbstdatenschutz im vernetzten Fahrzeug“[1] als Grundlage für die Entwicklung von Ansätzen und Schutzmaßnahmen in SeDaFa.

[1] SeDaFa Anforderungsanalyse für Selbstdatenschutz im vernetzten Fahrzeug. 2017 – Technischer Bericht.

2 Allgemeines Angreifermodell der IT-Security

Ein Angreifer beschreibt eine Instanz (bzw. eine Person), welche eine unautorisierte Handlung, d.h. einen Angriff, gegen ein System durchführt, die im Erfolgsfall zur Verletzung eines Schutzzieles führt. Ein Angreifermodell (oder Angriffsmodell) beschreibt daher die Attribute angenommener Angreifer, die bei der Sicherung eines Systems berücksichtigt werden. Es bildet die Grundlage für die Sicherheitsbewertung eines zugrundeliegenden Systems.

Das Angreifermodell aus der Perspektive der IT-Sicherheit beschreibt in der Regel sowohl den möglichen Angreifer, als auch den Angriff und die Angriffsvektoren. Es wird in der Regel in Zusammenarbeit zwischen Systemverantwortlichen und IT/IT-Sicherheits-Experten ermittelt. Die Aufstellung erfolgt zumeist im Kontext einer umfangreichen Risiko- und Bedrohungsanalyse und dient als eine Entscheidungsgrundlage bezüglich des für Sicherheitsmaßnahmen zu investierenden Aufwands.

Das Angreifermodell kann in seiner Ausprägung und dem Detaillierungsgrad variieren und nahezu beliebig aufwendig werden. Im Folgenden wird eine Übersicht über mögliche Klassifizierungen im Rahmen des Angreifermodells gegeben. Das umfasst sowohl die Klassifizierung der Angreifer als auch die Klassifizierung der Angriffe. Die Klassifizierung der Angreifer wird durch Beschreibung unterschiedlicher Arten von Angreifern vorgenommenin Abschnitt (Abschnitt 2.1). Die Klassifizierung potentieller Angriffe erfolgt anschließend durch die Beschreibung unterschiedlicher Ziele eines Angriffs (Abschnitt 2.2) und unterschiedlicher Arten eines Angriffes (Abschnitt 2.3). Eine beispielhafte Beschreibungen typischer Angriffe schließt die Klassifizierung ab (Abschnitt 2.4).

2.1 Klassifizierung der Angreifer

Zentraler Bestandteil des Angreifermodells ist die Übersicht und qualitative Beschreibung möglicher Angreifer hinsichtlich ihrer Motivationen, Ziele und Möglichkeiten. Abhängig von der Motivation der Angreifer, deren Know-How und den ihnen zur Verfügung stehenden Ressourcen stellen Angreifer unterschiedliche Gefährdungen dar. Im Rahmen der Gestaltung eines Schutzkonzeptes ist es unabdingbar, mögliche Angreifer ausreichend genau zu identifizieren. Auf dieser Grundlage kann dann entschieden werden, gegen welchen Arten von Angreifern die zu definierenden Schutzkonzepte standhalten müssen. Die nachfolgende Tabelle klassifiziert einige der in der IT-Sicherheit häufig beschriebenen Angreifertypen und soll aufzeigen, welche unterschiedlichen Ausprägungen ein möglicher Angreifer mit sich bringen kann.

Angriffe können auf der einen Seite von Angreifern wie *Hackern* ausgehen, die versuchen vorhandene Schwachstellen auszunutzen. Auf der anderen Seite können Bedrohungen jedoch auch von „*legitimen Angreifern*“ ausgehen. Ein Beispiel hierfür ist der Fahrzeughalter, der mittels Chiptuning die Leistung seines Fahrzeugs steigert.

Bezeichnung	Motivation	Know-how	Ressourcen
Skriptkiddie	• Langeweile, gepaart mit jugendlichem Leichtsinn • Spieltrieb u. Neugier • Streben nach Anerkennung • Vandalismus	• nicht unbedingt technisch versiert • bei DDoS Angriffe häufig organisierter	• frei verfügbare Exploits/ Rootkits • viel Zeit
Hacker	• Experimentierfreude • subjektiver Gerechtigkeitssinn und Selbstjustiz • Informationsfreiheit • Streben nach Anerkennung • höhere Ziele	• technisch sehr versiert • tiefreichendes Computergrundwissen • entwickelt eigene bzw. neue Exploits	• starke Community mit regem Wissensaustausch • hohe verteilte Rechnerleistung u. Bandbreite durch Community
Cracker	• Profitgier • persönliche Vorteile • Schädigung Dritter	• technisch sehr versiert • tiefreichendes Computergrundwissen • entwickelt eigene bzw. neue Exploits	• gehört unter Umständen der Hacker Community an • Bot-Netze
Mitarbeiter	• Frust • Rachegelüste • Profitgier • persönliche Vorteile • Vertuschung • Mobbing	• nicht unbedingt technisch versiert • Insiderwissen	• frei verfügbare Exploits/ Rootkits • bereits vorhandener (physischer) Zugang/ Zugriff
Wettbewerber	• Gewinnstreben • Wettbewerbsvorteil • Industrie- u. Unternehmensspionage • Sabotage	• nicht unbedingt technisch versiert	• hohes Budget • beauftragter Cracker
Krimineller	• Profitgier • Machtgier	• hoher Organisationsgrad • technisch versiert bis sehr versiert	• hohes Budget • beauftragten Cracker • greift auf eigene Entwickler zurück
Geheimdienst/ Regierung	• Wirtschaftsspionage • Verbrechensbekämpfung • Gewinnung von Erkenntnissen zur innen-, außen- und sicherheitspolitischen Lage • politische Intervention • Aufklärung, Vergeltung, und Abwehr • Sabotage	• hoher Organisationsgrad • technisch sehr versiert • tiefreichendes Computergrundwissen	• hohes Budget • viel Manpower • hohe technische Ausstattung • beauftragten Cracker • Zusammenarbeit mit Hacker • Legislative

2.2 Zielsetzung des Angriffs

Neben der Klassifizierung der Angreifer ist die Klassifizierung möglicher Angriffe erforderlich. Im Folgenden wird zur Klassifizierung eines Angriffes zunächst die Zielsetzung des Angriffs betrachtet.

Kategorisiert man mögliche Angriffsszenarien, die den Betrieb des ITS gefährden bzw. die zu einem Scheitern des Feldversuchs führen können, so sind im Wesentlichen drei Klassen von Szenarien zu unterscheiden. Sie zielen die Übertragung falscher Daten, die Sabotage des Systems oder den unbefugten Zugriff auf Daten. Mögliche Angriffe aus diesen Klassen sind im Folgenden aufgeführt:

1. **Übertragung falscher Daten**
   a) Angriffsszenario „Verfälschung übertragener Nachrichten“
   b) Angriffsszenario „Impersonation anderer Teilnehmer“
   c) Angriffsszenario „Selektive Unterdrückung von Nachrichten“
   d) Angriffsszenario „Selektive Verzögerung von Nachrichten“
   e) Angriffsszenario „Infektion des Systems mit Malware“
   f) Angriffsszenario „Veränderung von Daten in der Versuchszentrale“
   g) Angriffsszenario „Feldversuch mit inkonsistenter Software“

2. **Sabotage des Systems**
   a) Angriffsszenario „Jamming des Funkkanals“
   b) Angriffsszenario „Überlastung des Systems“
   c) Angriffsszenario „Sabotage des Routings“

3. **Unbefugter Zugriff auf Daten**
   a) Angriffsszenario „Abhören von Kommunikation“
   b) Angriffsszenario „Auflösen der Basisidentität“
   c) Angriffsszenario „Zuordnung mehrerer Pseudonyme“

2.3 Art des Angriffs

Für eine genaue Beschreibung des Angriffs wird hier nach der Beschreibung unterschiedlicher Zielsetzungen auch nach verschiedenen Arten der Angriffe unterschieden. Bei den nachstehenden Unterscheidungsmerkmalen handelt es sich um eine Unterscheidung der Angriffe nach den Kategorien aktiven/passiv, regional/überregionalen, böswillig/rationalen, als Insider Außenseiter, direkt/indirekte und einstufig/mehrstufig. Einen besonderen Aspekt stellt darüber hinaus auch die Angriffsfläche dar, welche ebenfalls zur Beschreibung der Art des Angriffs gezählt werden kann.

2.3.1 Aktiv / Passiv

Passive Angriffe betreffen die unautorisierte Informationsgewinnung und zielen auf den Verlust der Vertraulichkeit ab. Hier wird hauptsächlich auf die Informationsbeschaffung abgezielt. Der Angreifer sendet selbst keinerlei Daten. Er verhält sich sehr passiv, indem er lediglich den Datenverkehr anderer Teilnehmer belauscht, ohne diesen aktiv zu verändern. Damit erhält er wichtige Vermittlungs- und Benutzerinformationen. Das dient ihm z.B. dazu, Verkehrsflussanalyse des Netzes durchzuführen und somit einen Einblick über die Struktur eines Netzwerkes zu bekommen. Sämtliche abgefangenen Informationen könnten ihm als Ausgangsbasis für einen aktiven Angriff dienen.

Aktive Angriffe betreffen die unautorisierte Modifikation von Datenobjekten und richten sich somit gegen die Datenintegrität oder Verfügbarkeit eines Systems. Aktive Angriffe gehen daher über ein passives Beobachten hinaus und beinhalten aktive Eingriffe in die Kommunikation, um Dateien, IT-Systeme oder Benutzer zu manipulieren. Diese Art von Angriffen beinhaltet folglich die nicht autorisierte Modifikation von Daten und richtet sich somit in erster Linie gegen die Datenintegrität und die Verfügbarkeit. Nach der erfolgreichen Durchführung eines aktiven Angriffes hat der Angreifer direkten Zugang zu fremden Betriebsmitteln und kann diese aktiv missbrauchen. So kann er durch Wiederholung, Verzögerung, Einfügung, Modifikation und Löschung bestimmter Daten eine falsche Identität vortäuschen und eventuell Rechte und Attribute modifizieren.

2.3.2 Regional / Überregional

Ein *regionaler Angreifer* ist in seinem Handlungsspielraum auf einige wenige in seine Gewalt gebrachte Geräte oder Infrastruktureinheiten beschränkt.

Ein *überregionaler Angreifer* hat dagegen die Kontrolle über mehrere Geröte oder Infrastruktureinheiten, die über ein überregionales Netzwerk verteilt sind.

2.3.3 Böswillig / Rational

Ein *böswilliger Angreifer* strebt nicht nach persönlichen Vorteilen, sondern zielt darauf ab, den Mitgliedern zu schaden oder die Funktion des Systems zu beeinträchtigen. Es ist ihm zuzutrauen, dass er jedes mögliche Mittel einsetzt, ungeachtet der Kosten und Konsequenzen.

Im Gegensatz dazu strebt ein *rationaler Angreifer* nach persönlichem Profit und ist daher vorhersehbarer in Bezug auf Angriffsziele und Angriffsmittel.

2.3.4 Insider / Außenseiter

Ein Angreifer wird als *Insider* bezeichnet, wenn er ein authentifiziertes Mitglied des Systems ist, das mit anderen Mitgliedern kommunizieren kann.

Ein Angreifer wird als *Außenseiter* bezeichnet, wenn er von anderen Mitgliedern als unautorisierter Eindringling betrachtet wird. Dadurch ist er in der Vielfalt seiner Angriffe eingeschränkt.

2.3.5 Direkt / Indirekt

Ein direkter Angriff ist dadurch gekennzeichnet, dass dieser nur von einem einzigen Akteur ausgeführt wird, nämlich dem Angreifer. Dieser versucht eine Schwachstelle innerhalb einer Anwendung auszunutzen, um darüber vertrauliche Daten zu stehlen (Schutzziel Vertraulichkeit), Inhalte zu manipulieren (Schutzziel Integrität) oder andere Schäden zu verursachen.

Für die Durchführung eines *indirekten Angriffs* nutzt der Angreifer einen Benutzer des Zielsystems, welcher in der Regel bereits am Zielsystem angemeldet ist. Die Unwissenheit des Nutzers wird genutzt, um über dessen Rechte Zugriffe auf weitere Systeme zu erlangen.

(a) Direkter Angriff

(b) Indirekter Angriff (“Cross-Site-Angriff”)

Abbildung 2.1: Gegenübersetllung direkter / indirekter Angriff [1]

[2]

2.3.6 Einstufig / Mehrstufig

Mehrstufige Angriffe kombinieren verschiedene Angriffsarten, um sich dem eigentlichen Ziel schrittweise zu nähern. Hier kann z.B. zunächst zentrale Sicherheitsinfrastrukturen kompromittiert werden, um dann in weiteren Schritten die eigentlichen Ziele anzugreifen. Dazu noch ein Beispiel: Ein Angreifer nützt eine einfache, unwichtige Applikation, um zuerst einmal ins Intranet zu gelangen. Im zweiten Schritt dann wird versucht, von dort aus auf die datenführenden Systeme zu kommen. Benötigt ein Angriff nur einen einzelnen Schritt, um das geplante Ziel anzugreifen, so handelt es sich um *einstufigen Angriff*.

[2] Rohr, Rohr Sicherheit von Webanwendungen in der Praxis - Wie sich Unternehmen schützen können – Hintergründe, Maßnahmen, Prüfverfahren und Prozesse. 1. Auflage. Berlin Heidelberg New York: Springer-Verlag, 2015, ISBN 978–3–658–03851–9.

2.3.7 Angriffsfläche

Unter der Angriffsfläche („Attack Surface“) können verschiedene Bestandteile, wie z.B. Ziel, Aktivator, Protokoll und Kanal, verstanden werden. Für dieses Dokument werden unter der Angriffsfläche zur Begrenzung der Komplexität zunächst nur die Kanäle betrachtet, über die sich ein Angreifer Zugang zum System verschaffen kann. Im wesentlichen lässt sich hier unterscheiden, ob ein Angreifer physikalischen Zugriff auf ein System benötigt, oder ob ein Angriff auch über einen Kanal aus der Ferne (remote) durchgeführt werden kann.

2.4 Beispiele möglicher Angriffe

Unter den Beispielen möglicher Angriffe werden fünf konkrete Angriffsszenarien erläutert. Eine solche Kurzbeschreibung eines konkreten Angriffsszenarios dient dazu, ein gemeinsames Verständnis zu schaffen und geeignete Schutzmaßnahmen für ein konkretes Angriffsszenario zu definieren.

2.4.1 Maskierung

Bei einer Maskierung verdeckt der Angreifer seine eigene Identität durch eine andere bzw. eine gefälschte Identität. Tritt ein Angreifer als rechtmäßiger Knoten im Fahrzeugnetzwerk auf, dann kann er im Vergleich zu Außenseitern mehr Angriffsvarianten durchführen. Als Mitglied ist es ihm beispielsweise möglich, falsche Nachrichten zu erzeugen. Schutz gegen Maskierung bietet das Sicherheitsziel *Identitätsauthentifizierung*.

2.4.2 Manipulation

Bei der Nachrichtenmanipulation versucht ein Angreifer die Kommunikation ausgetauschter Nachrichten zu verändern. Verändert ein Angreifer verkehrssicherheitskritische Nachrichten, dann kann er dadurch erheblichen Schaden verursachen. Angreifer, die Nachrichten manipulieren, sind den Klassen „Insider“ und „Aktiver Angreifer“ zuzuordnen (siehe Abschnitt 2.3). Ansonsten bleibt es offen, ob sie böswillig oder rational handeln. Schutz gegen Manipulation bietet das Sicherheitsziel *Integritätsnachweis*.

2.4.3 Angriff mit Aufzeichnungswiederholung

Bei einem Angriff mit Aufzeichnungswiederholung zeichnet ein Angreifer einen Kommunikationsablauf auf und spielt den gesamten Ablauf oder Teile davon zu einem späteren Zeitpunkt ab. Die Durchführung dieses Angriffes ist nur einem aktiven Angreifer möglich. Ob er böswillige oder rationale Absichten hat, bleibt erneut offen. Schutz gegen solche Angriffe bietet das Sicherheitsziel *Aktualitätskontrolle*.

2.4.4 Verletzung der Privatsphäre

Verletzung der Privatsphäre bedeutet, dass ein Angreifer unberechtigt an Informationen und Daten über Fahrzeuge oder Fahrer gelangt. Dies können Informationen über die Identität des Fahrers, das Fahrverhalten oder die erreichten Orte sein. Schutz gegen die Verletzung der Privatsphäre bietet das Sicherheitsziel *Anonymität*.

2.4.5 Krimineller Missbrauch und Verleugnung

Angreifer mit böswilligen oder rationalen Absichten missbrauchen in vielen Fällen Informationen für kriminelle Zwecke. Da sie sich dadurch strafbar machen, versuchen sie ihre Identität zu verschleiern, um hinterher den Missbrauch zu verleugnen. Um dem entgegenzuwirken, muss ein Widerruf des Schutzes der Privatsphäre möglich sein.

3 Angreifermodell in SeDaFa

Da der Hauptfokus des Projektes SeDaFa auf Selbstdatenschutz liegt, muss das in Kapitel 2 dargestellte „klassische“ Angreifermodell aus dem Bereich der IT-Sicherheit nun auf das Projekt zugeschnitten werden. Typische Angreifermodelle für die IT-Sicherheitsbetrachtung beschreiben in der Regel nicht zulässige Zugriffe (z.B. durch Hacker). Im Bereich des Selbstdatenschutzes ist der Fokus leicht verschoben, da hier auch vertraglich vereinbarte und damit zulässige Zugriffe auf Daten bzw. Informationen von großer Relevanz sind. Im Angreifermodell sollen daher alle relevanten Akteure aufgezählt werden, denen ein Interesse an den Daten des Fahrzeugnutzers und des Fahrzeugs zugeordnet werden kann. Auch wenn die Akteure teilweise völlig legal auf Daten zugreifen, muss ermittelt werden, welche Risiken sich aus der Informationssammlung und -verarbeitung für den Fahrzeugnutzer bzw. den Fahrzeugbesitzer ergeben. Ziel des Angreifermodells ist damit die Identifizierung von Bedrohungen, die sich aus der Erhebung, Speicherung und Verarbeitung von Daten ergeben.

Eine solche Betrachtung ist auch aus datenschutzrechtlicher Sicht geboten. Art. 25 der DSGVO verlangt angemessene technische und organisatorische Maßnahmen zur Wahrung der Grundsätze des Datenschutzes. Diese Grundsätze finden sich insbesondere in Art. 5 DSGVO. Es handelt sich unter anderem um Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. Diesen Grundsätzen ist gemein, dass sie die betroffene Person vor dem Verantwortlichen schützen. Ein Angreifermodell für Zwecke des Datenschutzes muss daher auch die datenverarbeitende Organisation selbst analysieren. Sie ist es, die nicht ausreichend Transparenz herstellt, Zwecke überdehnt, zu viele Daten erhebt oder zu lange speichert und nicht ausreichende Maßnahmen zur Sicherung von Integrität und Vertraulichkeit trifft. Durch diesen veränderten Blickwinkel unterscheidet sich ein Angreifermodell für den Datenschutz von einem Angreifermodell, welches nur für Zwecke der IT-Security erstellt wird.

Das Vorgehen zur Ermittlung des Angreifermodells sieht im Rahmen von SeDaFa folgende Schritte vor: Zunächst werden die von einem Angriff betroffenen Daten und Personen klassifiziert (Abschnitt 3.1). Anschließend werden potentielle Angreifer ermittelt (Abschnitt 3.2) und ihre Ziele beschrieben (Abschnitt 3.3). In einem letzten Abschnitt werden schließlich unterschiedliche Arten eines Angriffs dargestellt (Abschnitt 3.4).

3.1 Klassifizierung relevanter Daten und Betroffener

3.1.1 Daten

Die Klassifizierung der relevanten Daten wird im SeDaFa-Dokument „Anforderungsanalyse für Selbstdatenschutz im vernetzten Fahrzeug“[1] im Kapitel zur Datentaxonomie genauer behandelt. Im Folgenden werden beispielhafte Daten aufgelistet, die sich aus den Anwendungsfällen ergeben:

- **Ereignisdaten:** Daten, die kurz vor und während eines Unfalls im Event Data Recorder (DER) gespeichert werden (Auslösen des Airbags, Gurtstraffungen, Lenkradwinkel, Geschwindigkeit).
- **Fahrverhalten:** Flüchtige Betriebsdaten, die während der Fahrt anfallen.
- **Synchronisierte Daten:** Daten, die vom Fahrer z.B. über das Smartphone (Kontakte, Musik) oder über das Infotainmentsystem (favorisierte Sender) eingebracht werden (Privatleben/persönliche Interessen/Soziales, Kundenkontakte, Routen).
- **Position:** Daten, die Aufschluss geben über den aktuellen Standort des Fahrzeugs bzw. ein aufgezeichnetes Bewegungsprofil.
- **Bildaufzeichnungen:** Innenraumkamera, Rückfahrkamera, Außenspiegelkamera.
- **Bezahl- & Abrechnungsinformationen:** Im Rahmen des Elektrischen Ladens fallen Informationen über Lade- und Bezahlvorgänge an.
- **Umgebungsdaten:** Daten zu der Umgebung des Fahrzeugs (Außentemperatur oder Parkplätze in der Umgebung).

Jeder dieser Datentypen wird im Fahrzeug entweder im Fahrzeug generiert oder verarbeitet, für synchronisierte Daten ist dazu noch ein weiteres Gerät (z.B. Smartphone) des Fahrers involviert. Durch die Vielfalt der in SeDaFa betrachteten Daten ist ein umfassender Schutz aller Fahrzeugdaten notwendig. Da es keinen im Fahrzeug verarbeiteten Datentyp gibt, der im Angreifermodell nicht berücksichtigt wird, müssen folglich auch die in SeDaFa zu entwickelnden Schutzmaßnahmen umfassend gestaltet sein.

[1] SeDaFa Anforderungsanalyse für Selbstdatenschutz im vernetzten Fahrzeug. 2017 – Technischer Bericht.

3.1.2 Betroffene

Unter dem Begriff „Betroffene“ werden in SeDaFa diejenigen Personen verstanden, die direkt von einer möglichen Offenlegung von Daten betroffen sind, da diese Daten Rückschlüsse auf die Person selbst zulassen oder im Rahmen der Aktivität einer solchen Personen entstanden sind. Folgende Personen können als Betroffene eingestuft werden:

- Fahrer
- Halter
- Eigentümer
- Mitfahrer
- Verkehrsteilnehmer
- Vorbesitzer
- Gesellschaft (z.B. bei Car2X)

Es gibt damit in SeDaFa deutlich mehr Entitäten, die potentiell von einem Angriff betroffen werden können. Ihnen allen ist gemeinsam, dass sie zum Fahrzeug in einem Nutzer-Verhältnis stehen. Demgegenüber sind bei den potentiellen Angreifern auch Entitäten außerhalb dieses Nutzer-Verhältnisses zu betrachten (z.B. solche, die zum Fahrzeug in einem Dienstleister-Verhältnis stehen).

3.2 Klassifizierung der Angreifer

Viele der in Abschnitt 3.1 genannten Daten sind für potenzielle Angreifer von Interesse. Angreifer können im Kontext von SeDaFa daher all jene Personen oder Institutionen sein welche Zugriff auf Fahrzeugdaten erhalten oder Interesse daran haben. Dabei handelt es sich nicht nur um Angreifer im klassischen Sinne, sondern größtenteils um Entitäten, die an einem Prozess der Datenverarbeitung beteiligt sind und die (aus unterschiedlichen Gründen) Interesse an den Daten haben. Das Interesse der jeweiligen Entitäten bezieht sich dabei auf die Möglichkeit, Daten einzusehen und weiterverwenden zu können. Die folgenden Entitäten könnten in diesem Sinne Angreifer sein:

- Fahrzeugführer (Fahrer)
- Fahrzeughalter (Besitzer)
- Insassen
- Gegner der Fahrzeuginsassen/ des Halters
- Straftäter
- Fahrzeughersteller (OEM)
- Konkurrierende Fahrzeughersteller
- Zulieferer
- Werkstatt
- Carsharing Anbieter
- Telekommunikationsunternehmen
- Staat (z.B. Strafverfolgungsbehörden / Polizei)
- Versicherungsunternehmen
- Automobilclubs (ADAC, ACE, AvD, VCD, BAVC)
- Anbieter von Informationsdiensten
- Anbieter von Unterhaltungsdiensten
- Kreditinstitute, Banken, Leasinggeber
- Portalanbieter (Google, Apple)
- Werbewirtschaft

Speziell in der Elektromobilität gibt es eine Fülle an Entitäten, die am elektrischen Laden beteiligt sind. Sie erhalten ebenfalls Zugriff auf eine Vielzahl an Ladedaten, Positionsdaten und Beizahlinformationen. Bei den Beteiligten handelt es sich um die folgenden Akteure:

- Certification Authority
- Billing & Payment Clearinghouse
- Vehicle Service
- Roamingpartner Mobility Operator
- Grid Operator
- Stromlieferant Energy Provider
- Charge Spot (Ladesäule)

- Eigentümer der Batterie
- Betreiber des Ladepunktes
- Plattformanbieter (Ladenetz, Hubject, e-clearing.net u.a.)

Die Anzahl und Variabilität potentieller Angreifer zeigt, dass im Gegensatz zu einem klassischen Angreifermodell die Anzahl und Eigenart von Angreifern nicht eng auf spezielle Fälle zugeschnitten werden kann, sondern stark vom betrachteten Nutzungsszenario und den dort beteiligten Akteuren abhängt. Darüber hinaus wird deutlich, dass jeder im Fahrzeugkontext beteiligte Aktuer zum potentiellen Angreifer werden kann. Insbesondere zeigt die Überschneidung der potentiellen Angreifer mit den in Abschnitt 3.1.2 genannten Betroffenen, dass ein Akteur in bestimmten Szenario als Angreifer, in einem anderen dagegen als Betroffener fungieren kann. Durch diesen starken Kontextbezug verbieten sich in SeDaFa somit monoschematische und stereotype Angreiferklassifikationen. Sowohl die potentiellen Angreifer als auch die notwendigen Schutzmaßnahmen müssen damit für jeden Anwendungsfall separat betrachtet werden.

3.3 Zielsetzung des Angriffs

Während das Angreifermodell sich in Bezug auf potentielle Angreifer und Betroffene stark von einem klassischen Angreifermodell unterscheidet, herrscht in Bezug auf die Ziele der Angreifer eine große Deckungsgleichheit zum klassischen Angreifermodell vor. Alle in Abschnitt 2.2 genannten Zielsetzungen von Angriffen sind auch für SeDaFa relevant. Auf eine Wiederholung der dort genannten Angriffsziele wird daher hier verzichtet. Stattdessen soll im Folgenden die Motivation unterschiedlicher Angreifer genauer klassifiziert werden. Dafür wird in der nachstehenden Tabelle eine Zuordnung zwischen Daten, Angreifern und deren Motivation vorgenommen. Je nach Datentyp sind somit unterschiedliche Angreifer mit und unterschiedlichen Angriffszielen vorstellbar:

Ereignisdaten:

Interessenten	Motivation
OEM/Zulieferer	Produktbeobachtungen (Fehlfunktionen einsehen, technische Optimierung), Abwehr von Ansprüchen
Strafverfolgungsbehörden (Polizei), Versicherung	Rekonstruktion von Unfällen zur Identifizierung von Verantwortlichen und Aufklärung von Straftaten
Werkstatt	Rückschlüsse auf Defekte finden

Fahrverhalten:

Interessenten	Motivation
OEM/Zulieferer	Produktbeobachtungen (statistische Analysen von Verschleißteilen für technische Optimierungen), Erfindungen/Patente, Kundenanalyse, gezielte Werbung
Zulieferer	Verschleißanalyse des Akkus, Erfüllung von vertraglichen Vorgaben
Händler	Abwehr von Ansprüchen
Leasinggeber	Nach fehlender Ratenzahlung ggf. Positionsbestimmung bzw. Sperrung des Fahrzeugs
Versicherung, Strafverfolgungsbehörden	Rückschlüsse auf Zustand des Fahrers (z.B. bei Sekundenschlaf, Schlingern)
Car Sharing Anbieter/Autovermietung	Fahranalyse des Mieters und ggf. Strafen bzw. höhere Tarife
Versicherungen	Score-Werte ermitteln, Abwehr von Schadensersatzansprüchen
Werkstatt	Ferndiagnose
Werbeindustrie	Personalisierte Werbung aufgrund von Füllständen
Staat	Gefahrenabwehr, Umweltentlastung, Verkehrseffizienz
Arbeitgeber	Verhaltens- und Leistungskontrolle

Synchronisierte Daten:

Interessenten	Motivation
OEM	Kundenanalyse
Werbeindustrie	Auf Basis von privaten Daten gezielt Werbung schalten, Datenhandel
Neider	Ansehen schädigen.
Konkurrenz	Kundenkontakte untergraben, Kundenadressen ausfindig machen, Konditionen einsehen

Position:

Interessenten	Motivation
Werbeindustrie	Ortsbezogene Werbung, POI
Car Sharing Anbieter/Autovermietung	Geofencing aufgrund von Vertragsbedingungen.
Fahrer	Überwachung einzelner Familienangehöriger (Ehepartner, Kinder), Neugier
Straftäter	Fahrzeugdiebstahl, Einbruch
Staat	Mauterhebung, Überwachung
	Datenhandel

Bildaufzeichnung:

Interessenten	Motivation
Werbeindustrie	Ortsbezogene Werbung, POI
Car Sharing Anbieter/Autovermietung	Geofencing aufgrund von Vertragsbedingungen.
Fahrer	Überwachung einzelner Familienangehöriger (Ehepartner, Kinder), Neugier
Straftäter	Fahrzeugdiebstahl, Einbruch
Staat	Mauterhebung, Überwachung
	Datenhandel

Umgebungsdaten:

Interessenten	Motivation
Werbeindustrie	Ortsbezogene Werbung, POI
Car Sharing Anbieter/Autovermietung	Geofencing aufgrund von Vertragsbedingungen.
Fahrer	Überwachung einzelner Familienangehöriger (Ehepartner, Kinder), Neugier
Straftäter	Fahrzeugdiebstahl, Einbruch
Staat	Mauterhebung, Überwachung
	Datenhandel

3.4 Art des Angriffs

Wie schon bei den Angriffszielen gibt es auch bei den in SeDaFa betrachteten Angriffsarten eine starke Entsprechung zum klassischen Angreifermodell. Die in SeDaFa berücksichtigen Angriffsarten unterscheiden sich somit nicht von den in Abschnitt 2.3 genannten Arten von Angriffen. Alle dort genannten Arten von Angreifern sind auch im Umfeld des vernetzten Fahrzeug möglich:

- Aktive und passive Angreifer
- Regionale und überregionale Angriffe
- Böswillige und rationale Angriffe
- Angreifer als Insider oder als Außenseiter
- Direkte oder indirekte Angriffe
- Einstufige oder mehrstufige Angriffe
- Angriffe mit stark variierender Angriffsfläche

Insbesondere im Hinblick auf die „Angriffsfläche“ lassen sich jedoch weitere Konkretisierungen vornehmen. Wie in Abschnitt 2.3 definiert, werden dabei die Möglichkeiten bzw. Kanäle betrachtet, über die ein Angreifer sich möglicherweise

Zugriff auf das Fahrzeug verschaffen kann. Hierbei wird zwischen physikalischem und drahtlosem Zugriff auf das Fahrzeug unterschieden und weiteren Zugriffsmöglichkeiten bzw. angrenzende Systemen, an denen Daten abgegriffen werden können oder die als Startpunkt eines Angriffs dienen.

- Physikalischer Zugriff
  - Steuergeräte
  - Bordnetzkommunikation
  - OBD-Schnittstelle
  - Bedienelemente (z.B. Headunit)
  - CD/USB/SD
- Drahloser Zugriff
  - Short Range: Wifi, Bluetooth, NFC, proprietäre Protokolle (z.B. RKE)
  - Long Range: GSM, Mobilfunk
- Weitere Zugriffsmöglichkeiten
  - Zugriff auf Kommunikationskanal zwischen Fahrzeug und Backend
  - Zugriff auf Kommunikationskanäle zwischen Severn verschiedener Anbieter (z.B. Datenmarkplätze)
  - Zugriff auf Smartphone/Laptop des Nutzers
  - Zugriff auf IT der Werkstatt
  - Zugriff auf Car2X Infrastuktur
  - Zugriff auf Daten im Backend
    - Berechtigt durch Unternehmenshierarchie
    - Unberechtigter Zugriff (Hacker, etc.)

Es gibt damit zahlreiche Möglichkeiten als Ansatzpunkt eines Angriffs. Die Angriffsfläche hängt jedoch stark vom Kontext (Angreifer und Ziel des Angriffs) ab. In SeDaFa muss die Angriffsfläche daher immer im Zusammenhang mit speziellen Nutzungsszenarien betrachtet werden.

4 Fazit

In SeDaFa sollen neue Wege für den Selbstdatenschutz durch Fahrzeugnutzer entwickelt werden. Dazu wurde in diesem Dokument ein Angreifermodell erarbeitet, das als Basis für die in SeDaFa entwickelten Schutzmaßnahmen und Werkzeuge zum Schutz der im vernetzten Fahrzeug anfallenden Daten dient. Erst auf der Basis dieses Angreifermodells können Anforderungen an Schutzmaßnahmen abgeleitet und Werkzeuge für den Selbstdatenschutz entworfen werden.

In diesem Dokument wurde zunächst ein allgemeines Angreifermodell vorgestellt, wie es in der IT-Security häufig zu finden ist (Kapitel 2). Dabei blieb der Kontext des vernetzten Fahrzeugs jedoch noch im Hintergrund. Auf dieser Basis wurde anschließend ein Angreifermodell entwickelt, das auf das in SeDaFa betrachtete vernetzte Fahrzeug zugeschnitten ist (Kapitel 3). Durch die speziellen Anforderungen im Bereich Selbstdatenschutz ergeben sich dabei Abweichungen zum klassischen Angreifermodell, die besondere Anpassungen erfordern. Dies zeigt sich vor allem in der Klassifizierung von Angreifern sowie den von einem Angriff betroffenen Daten und Personen. In anderen Bereichen dagegen entspricht das in SeDaFa zugrunde gelegte Angreifermodell stark dem allgemeinen Angreifermodell der IT-Sicherheit. Starke Überschneidungen finden sich etwa in Bezug auf die Arten von Angriffen oder die Zielen eines Angreifers.

Durch die große Anzahl der im vernetzten Fahrzeug involvierten Akteure und Daten ergibt sich in SeDaFa eine sehr umfassende Betrachtung von Angreifern, ihren Methoden, Zielen und Motivationen sowie der betroffenen Daten und Entitäten. Diese Bandbreite an möglichen Angriffen, bei denen sich die Rollen von Angreifer und Betroffenem von Fall zu Fall ändern kann, erzwingt eine stark kontextabhängige Betrachtung. Das in diesem Dokument spezifizierte Angreifermodell muss daher zur Entwicklung der Schutzmaßnahmen jeweils auf die speziellen, in SeDaFa behandelten Anwendungsfälle angewendet werden.

Literaturverzeichnis

Rohr, Rohr: Sicherheit von Webanwendungen in der Praxis - Wie sich Unternehmen schützen können – Hintergründe, Maßnahmen, Prüfverfahren und Prozesse. 1. Auflage. Berlin Heidelberg New York: Springer-Verlag, 2015, ISBN 978–3–658–03851–9

SeDaFa: Anforderungsanalyse für Selbstdatenschutz im vernetzten Fahrzeug. 2017 – Technischer Bericht

SeDaFa

2. August 2017

SeDaFa-D1.5-1.0