Grundprojekt Bericht:

Architektur eines V2X Automotive Security Gateways

Sebastian Szancer

26. Oktober 2018

Fakultät Technik und Informatik

Department Informatik

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Zusammenfassung

Die Kommunikation moderner Fahrzeuge mit der Außenwelt spielt eine zunehmend größere Rolle. Neben physikalischen Schnittstellen, wie z.B. USB, besitzt das moderne Fahrzeug ein Connectivity-Gateway für "Over-The-Air"-Verbindungen, welche über unterschiedliche Technologien wie WLAN, Bluetooth, oder LTE und zukünftig auch 5G hergestellt werden. Über dieses Gateway wird das Fahrzeug zum Teilnehmer in diversen Netzwerken, wozu neben dem Internet vor allem VANETs für V2X Kommunikation zählen. Die Kommunikation über das Gateway muss entsprechend abgesichert werden. Dies passiert über ein Security-Gateway, welches Teil des Connectivity-Gateways ist. Diese Arbeit gibt einen Überblick über die externe Fahrzeug-Kommunikation und leitet ausgehend davon die Anforderungen an ein Automotive Security-Gateway ab. Dazu zählt neben funktionalen Anforderungen wie der Überprüfung des Datenverkehrs, kryptographischer Funktionalität, oder der Proxy-Funktion zwischen internen Diensten und der Außenwelt, die Echtzeitfähigkeit. In dieser Arbeit werden auch die Konzepte des Security-Gateways und des Intrusion Detection Systems aus der klassischen IT-Security vorgestellt. Basierend darauf wird eine Architektur für ein Automotive Security-Gateway entwickelt.

Inhaltsverzeichnis

1 Einleitung

Beim modernen Fahrzeug spielt die Kommunikation mit der Außenwelt eine zentrale Rolle. Neben physikalischen Schnittstellen wie USB oder OBD-II (On-Board Diagnostics) besitzt das moderne Fahrzeug ein Gateway für "OTA"-Verbindungen (Over-The-Air), welche über WLAN/Wi-Fi (IEEE 802.11), Bluetooth, UMTS (3G), LTE (4G) und zukünftig 5G hergestellt werden. Über dieses Gateway, Connectivity-Gateway [27] oder Central Communication Unit (CCU) [18] genannt, wird das Fahrzeug zum Teilnehmer in diversen Netzwerken. Neben dem Internet sind das vor allem VANETs für V2X Kommunikation [21].
Die Kommunikation über das Connectivity-Gateway muss abgesichert werden. Dies geschieht durch ein Security-Gateway, welches Teil des Connectivity-Gateways ist (Siehe: Abbildung 1). Das Ziel dieser Arbeit ist es, die Anforderungen an ein solches Security-Gateway, welche sich aus der externen Fahrzeug-Kommunikation ergeben, zu identifizieren und ausgehend davon eine Architektur für ein Security-Gateway im Automotive-Bereich zu entwickeln. Diese Security-Gateway Architektur sollte auch bestmöglich zu der für moderne Fahrzeuge vorgesehenen Dienst-basierten Architektur [19] kompatibel sein.
Diese Arbeit ist wie folgt aufgebaut: Abschnitt 2 gibt einen Überblick über die externe Kommunikation und Netzwerk-Architektur von modernen Fahrzeugen. Außerdem werden die relevanten Grundbegriffe Security-Gateway, Firewall und Intrusion Detection Systemen (IDS) aus der IT-Security eingeführt. In Abschnitt 3 werden verwandte Arbeiten vorgestellt und der Beitrag dieser Arbeit zum Security-Gateway zur Absicherung der externen Kommunikation im Automotive-Bereich unterstrichen. In Abschnitt 4 werden die Anforderungen an das Security-Gateway und die davon ausgehend entwickelte Architektur vorgestellt. Dabei wird im Detail auf das Intrusion Detection System, eine zentrale Komponente des Security-Gateways, eingegangen. Abschnitt 5 fasst diese Arbeit abschließend zusammen und bietet einen Ausblick auf weitere mögliche Arbeit zum Security-Gateway im Automotive-Bereich.

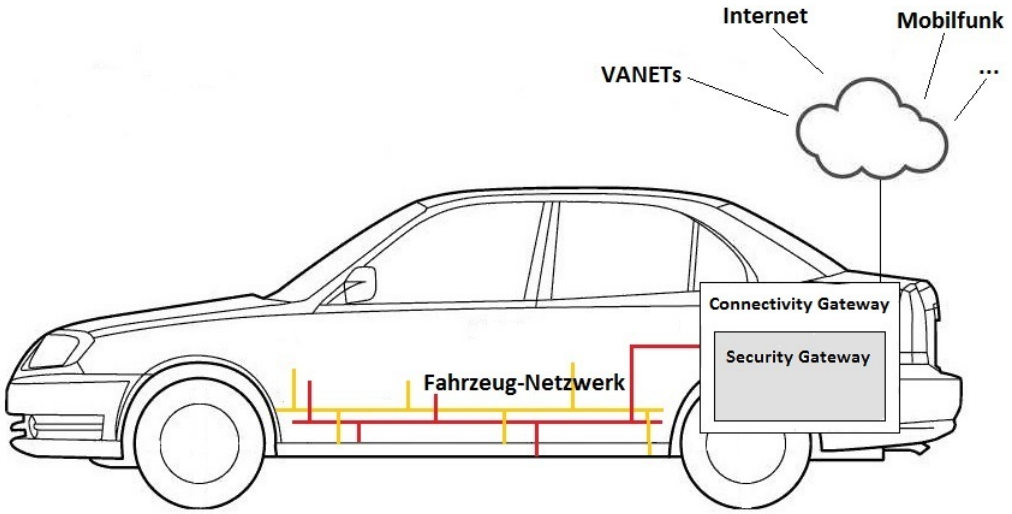

Abbildung 1: Schematische Abbildung: Fahrzeug mit Security-Gateway

2 Grundlagen

Dieser Abschnitt gibt einen Überblick über die Netzwerk-Architektur und die externe Kommunikation von modernen Fahrzeugen. Außerdem werden die Grundbegriffe Security-Gateway, Firewall und Intrusion Detection System (IDS) aus der IT-Security eingeführt.

2.1 IT-Security Grundbegriffe

2.1.1 Security-Gateway und Firewall

Die Begriffe "Security-Gateway" und "Firewall" werden in der Literatur nicht einheitlich verwendet. Oft wird unter einer Firewall "nur" ein Paketfilter mit Stateful Packet Inspection verstanden. Nach dieser Definition verhindern Firewalls nur Angriffe auf der Internet- und Transport-Schicht (OSI-Layer 3 und 4). Unter dem Begriff "Firewall" kann aber statt eines Paketfilters auch ein Application-Level-Gateway (ALG) verstanden werden [24], welches Angriffe auf der Anwendungsschicht verhindert (OSI-Layer 7) und eine Proxy-Funktion für zu schützende Dienste erfüllt.
Unter einem Security-Gateway versteht man in der Regel ein Device zur umfassenden Absicherung des Datenverkehrs, bestehend aus einem Paketfilter und einem ALG [6]. Somit bietet ein Security-Gateway Schutz auf der Internet-, Transport- und Anwendungsschicht (OSI-Layer 3, 4 und 7). Mehr dazu in Abschnitt 3. Der Begriff "Security-Gateway" wird allerdings manchmal auch gleichbedeutend mit dem Begriff "Firewall" verwendet [24].

2.1.2 Intrusion Detection System

Intrusion Detection Systeme (IDS) dienen der frühzeitigen Erkennung von Angriffen durch Analyse des Datenverkehrs im Netzwerk [24]. Generell unterteilt man Intrusion Detection Systeme in 2 Klassen: "Anomaly-based IDS" und "Speci-fication-based IDS" [22], auch bezeichnet als "Signature-based" oder "Rule-based" IDS [16]. Bei den Anomaly-based IDS werden Abweichungen vom Normalzustand, die auf einen Angriff hindeuten, erkannt. Ein Beispiel für eine Anomalie ist eine deutlich erhöhte Paketrate. Bei Specification-based IDS wird bspw. geprüft, ob Nachrichten einer gegebenen Spezifikation entsprechen. Auch wenn Angriffe nach bekannten Mustern verlaufen, können diese aufgrund der bekannten Muster (Spezifikation) erkannt werden. Eine weiter entwickelte Form eines IDS, welche IT-Angriffe nicht nur erkennt, sondern auch entsprechend reagiert, um sie zu vereiteln (z.B. Verwerfen aller Pakete von einer bestimmten Adresse), nennt man Intrusion Prevention System (IPS) [15] oder auch Intrusion Detection and Prevention System (IDPS).

2.2 Das moderne Fahrzeug

2.2.1 Fahrzeug-Netzwerk Architektur

Das moderne Fahrzeug-Netzwerk besteht aus etwa 50 bis 100 ECUs die über einen Real-Time Ethernet Backbone mit peripheren Bussystem-Netzen (z.B. CAN) [28] verbunden sind. Es gibt viele unterschiedliche ECUs die alle auf bestimmte Anwendungen spezialisiert und beschränkt sind (schematische Abbildung 2). Sie lassen sich in 5 Anwendungsbereiche aufteilen: Antrieb- und Fahrwerksteuerung, Infotainment, Wartung, Sicherheitselektronik und Komfort. Die Netzwerk-Fragmentierung spiegelt diese Aufteilung wieder: die ECUs sind nach Anwendungsbereich gruppiert und über Switche verbunden. Man bezeichnet diese Netzwerk-Architektur als Domain Architektur (Siehe: Abbildung 3). Eine Alternative zur Domain Architektur ist die Zonen Architektur, bei der nahe beieinander verbaute ECUs vernetzt werden, anstelle einer Vernetzung nach Domänen. Der Vorteil hierbei ist, dass das Netzwerk durch die Reduktion des Kabelsatzes einfacher, günstiger und leichter ist. Ein wichtiger Punkt bei der Zonen Architektur ist allerdings die Unterbindung unerlaubter Kommunikation zwischen ECUs verschiedener Anwendungsbereiche (z.B. zwischen Infotainment und Antrieb- und Fahrwerksteuerung). In der Literatur wird noch überwiegend von der Domain Architektur beim Fahrzeug-Netzwerk ausgegangen. Je nach Anwendung unterscheiden sich die Security-Anforderungen einer ECU; auch hinsichtlich der kryptographischen Funktionalität. So wird bspw. für das Connectivity-Gateway neben Vertraulichkeit und Integrität der Nachrichten auch Authentizität benötigt, weil mit der Außenwelt kommuniziert wird, während bspw. für ECUs aus dem Bereich Komfort Vertraulichkeit und Integrität vollkommen ausreichen. Im Rahmen des EVITA Projekts (https://www.evita-project.org/index.html) wurde die Realisierung der kryptographischen Funktionalität einer ECU durch eine spezielle Hardware-Komponente

vorgesehen, nämlich ein so genanntes Hardware Security Module (HSM) [1, 21]. Das HSM ist ein isoliertes Subsystem der ECU. HSMs werden generell in 3 HSM Security Level unterteilt: EVITA Light, EVITA Medium und EVITA Full. Diese bieten unterschiedliche Level an kryptographischer Funktionalität. Während sich bspw. EVITA Light nur auf symmetrische Verschlüsselung beschränkt, bietet EVITA Full neben symmetrischer Verschlüsselung auch hoch-performante und zeitkritische asymmetrische Verschlüsselung.

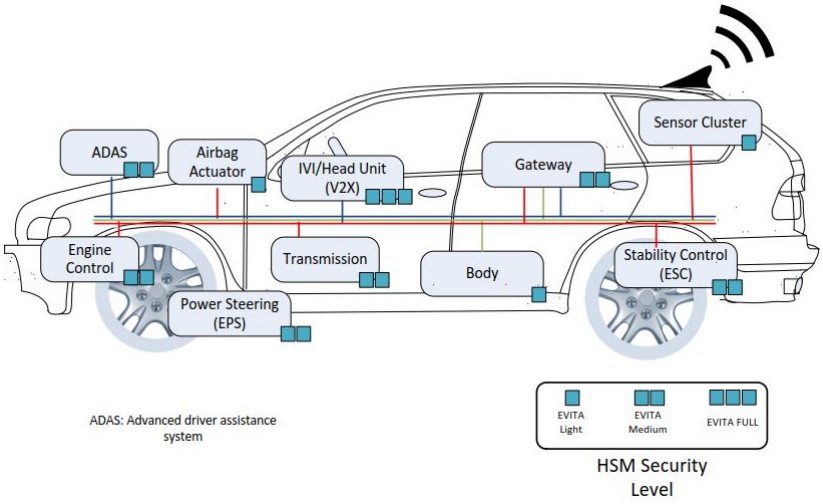

Abbildung 2: Übersicht: modernes Fahrzeug (Quelle: [21], S.13)

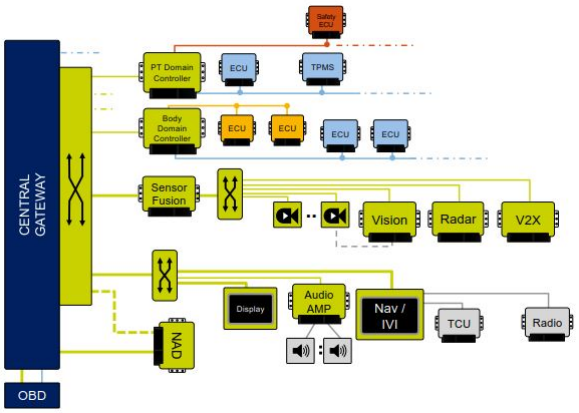

Abbildung 3: Domain Architektur mit Real-Time Ethernet Backbone (Quelle: [28], S.4)

Für zukünftige Fahrzeug-Netzwerk Architekturen wird eine Reduktion der Anzahl der ECUs und damit einhergehende Zentralisierung der Rechenleistung, sodass mehrere Software-Komponenten auf einer ECU ausgeführt werden, vorgeschlagen [9]. Neue Funktionalität wird dann nicht in Form von zusätzlichen ECUs, sondern in Form von neuen Software-Komponenten in das Fahrzeug integriert. Für die zugrunde liegende Software-Architektur ist der Ansatz der Service-Oriented Architecture (SOA) vorgesehen [9]. Bei einer SOA stellen Service Provider Dienste (Software und Hardware) bereit und Service Consumer nutzen diese Dienste. Eine lose Kopplung zwischen Providern und Consumern wird durch eine Middleware erreicht. Auch die Auslagerung von Diensten außerhalb des Fahrzeugs, bspw. von sehr Ressourcen-intensiven Diensten auf leistungsstarke Server, wird ein wichtiger Aspekt sein, was die Bedeutung des Connectivity-Gateways erhöhen wird.

2.2.2 Externe Fahrzeug-Kommunikation

Unter externer Fahrzeug-Kommunikation wird in dieser Arbeit jegliche Kommunikation über das Connectivity-Gateway mit der Außenwelt verstanden. Die Kommunikation über die physikalischen Schnittstellen (wie USB oder OBD-II) wird hier nicht betrachtet, da die beiden getrennt vom Connectivity-Gateway ablaufen [27, 28].
Für den Zweck der Entwicklung eines Security-Gateways soll eine Klassifizierung der externen Fahrzeug-Kommunikation vorgenommen werden. Eine erste grobe Aufteilung ist eine in Fahrzeug-bezogene (z.B. Abstandhalte-Assistent) und Fahrer-bezogene (z.B. Entertainment) Kommunikation [12]. Eine nächste Einteilung erfolgt nach dem Aufgabenbereich, in den die Kommunikation fällt. Beim modernen Fahrzeug sind das die 5 bekannten Aufgabenbereiche; im Kontext von Diensten spricht man auch von Service-Domains: Antrieb- und Fahrwerksteuerung, Infotainment, Wartung, Sicherheitselektronik (z.B. ABS, Airbag, Gurtstraffer) und Komfort (z.B. elektronische Fensterheber) [3, 26, 4]. Die externe Fahrzeug-Kommunikation fällt vor allem unter Antrieb- und Fahrwerksteuerung, Infotainment und Wartung, in Zukunft wahrscheinlich auch unter Sicherheitselektronik [17], während Komfort, obwohl in Einzelfällen ebenfalls denkbar, aktuell keine Rolle spielt. Innerhalb einer Domain ist die Kommunikation hinsichtlich wichtiger Eigenschaften, wie z.B. Echtzeitanforderung, weitgehend ähnlich [3], weshalb eine allgemeine Unterteilung nach Domains sinnvoll ist.
Wird ein Ansatz hierarchischer Informations-Architekturen verfolgt [20], kann zusätzlich zur Service-Domain auch die Hierarchie-Ebene der Information in einer solchen Architektur zur Klassifikation der externen Kommunikation hinzugezogen werden. Die Hierarchie kann ausgehend von unterschiedlichen Aspekten erstellt werden. Ein naheliegender Ansatz ist eine Hierarchie basierend auf der Service-Location von Informationen und Funktionen, die von Sensoren und Aktoren, über das Fahrzeug als Ganzes, bis hin zu Gruppen von Fahrzeugen reicht (Siehe: Abbildung 4). Die externe Fahrzeug-Kommunikation ist hierbei eher auf den oberen Ebenen angesiedelt. Ein weiterer Ansatz ist eine Hierarchie basierend auf dem Abstraktions-Level von Informationen und Funktionen, das von einfachen Signalen bis hin zu Wissen (z.B. "Abstand zum Auto vor mir beträgt 25m") und Verhalten (z.B. koordiniertes Fahren) reicht (Siehe: Abbildung 4). Die externe Fahrzeug-Kommunikation ist hierbei auf den Ebenen von "Data" (z.B.Audio-Stream) aufwärts und zukünftig vor allem auf den obersten Ebenen angesiedelt.

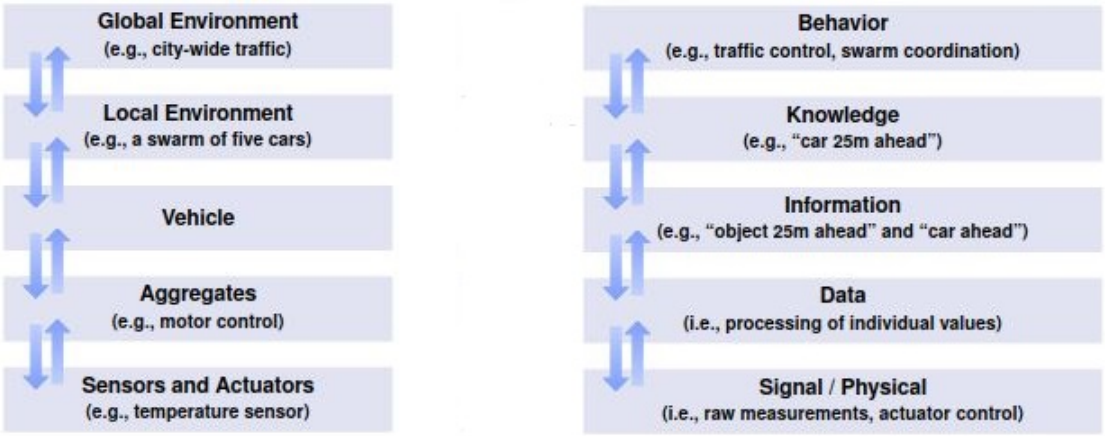

Abbildung 4: Hierarchische Informations-Architekturen (Quelle: [20], S.3 (abgeändert))

Es folgt ein kurzer Überblick über die aktuell im Auto vorhandene externe Kommunikation in den relevanten Bereichen Antrieb- und Fahrwerksteuerung, Infotainment und Wartung:

Antrieb- und Fahrwerksteuerung:
- V2E Kommunikation (z.B. autonomes Parken, Kommunikation mit Straßenschildern)
- Koordiniertes Fahren (V2V) (z.B. Abstand halten, Kolonne fahren)

Infotainment:
- Audio-Streams (z.B. Musik, Telefongespräche)
- Video-Streams
- integrierte Online Dienste (z.B. Wetter, Tankstellensuche, Emails)
- klassisches Surfen im Internet (via eingebautem Router im Auto)
- Navigation (z.B. Karten-Download)

Wartung:
- Over-the-Air ECU Updates
- (Fern-) Diagnose

Durch die zunehmende Vernetzung des Automobils [10, 8] wird die Bedeutung und der Umfang der Kommunikation des Fahrzeugs mit der Außenwelt zukünftig noch größer. Für eine abschließende Klassifikation externer Fahrzeug-Kommunikation wurden, ausgehend von den unterschiedlichen Service-Domains, die folgenden Eigenschaften identifiziert: Die beiden wichtigsten Eigenschaften sind, auch nach [3]:

Echtzeitanforderungen:
Hard real-time oder soft real-time?

Sicherheitsrelevanz:
Wie sicherheitskritisch ist der Dienst (z.B. V2V Kollisionsvermeidung vs. Email-Dienst)? Wie ist die Art des Zugriffs des Dienstes auf Speicher: ”Read” oder ”Read/Write”?

Weitere relevante Eigenschaften sind:

Datenmenge:
Paket-Größe und Paket-Rate

Authentizität:
Wie wichtig ist die Authentizität der Kommunikationspartner (z.B. ECU Software-Update vs. Musik-Stream) und wie gut lässt sich diese gewährleisten?

Kommunikations-Muster [13]:
Verbindungslos/verbindungs-orientiert, Message, Stream, Publish-Subscribe...

Service-Location [13]:
1) Dienst im eigenen Fahrzeug, oder Dienst außerhalb des eigenen Fahrzeugs und 2) über das Internet erreichbar (höhere Latenz), oder 3) über ein VANET erreichbar

Abschließend eine Übersicht der Service-Domains hinsichtlich der wichtigsten Eigenschaften:

Service-Domain	**Echtzeitanforderungen**	**Sicherheitsrelevanz**	**Datenmenge**
Antrieb- und Fahrwerksteuerung	hard real-time	hoch	gering
Infotainment	soft real-time	gering	hoch
Wartung	soft real-time	hoch	mittel

Tabelle 1: Service Domains nach Kommunikations-Eigenschaften

3 Verwandte Arbeiten

Dieser Abschnitt gibt eine Übersicht über ausgewählte Arbeiten, die sich mit Security-Gateways sowohl in der klassischen IT-Security, als auch im Automobil, oder mit der Erkennung von Anomalien in Fahrzeug-Netzwerken befasst haben.

In ihrer Arbeit *Automotive SIEM and Anomaly Detection Using Sand-Sprinkled Isolation Forest* befassen sich Haga et al. [14] mit der Erkennung von Anomalien im Fahrzeug-internen Netzwerk. In ihrem System erfolgt die Analyse der erfassten Fahrzeug-Netzwerk-Daten und die Erkennung von Anomalien auf Servern außerhalb des Fahrzeugs, da diese leichter zu warten sind und über eine größere Rechenleistung und mehr Speicher verfügen, als im Fahrzeug verbaute Rechner. Erkannte Anomalien werden zunächst nur gemeldet. Die Reaktion auf einen Angriff im Fahrzeug selbst erfolgt erst später in Form von Updates der ECUs. Als Algorithmus zur Anomalie-Erkennung wird Sand-Sprinkled Isolation Forest aus dem Bereich des Machine Learnings vorgeschlagen, da dieser hinsichtlich Speicher und Rechenleistung effizient ist. Der Algorithmus wird auf die Fahrzeug-Netzwerk-Daten angewendet, ohne dass der Automotive Kontext speziell berücksichtigt werden muss. Die Erkennung einer Anomalie erfolgt im Prinzip durch die Abweichung vom Durchschnitt einer Teilmenge der Trainingsdaten. Die Evaluierung der Anomalie-Erkennung ihrer Arbeit erfolgt über CAN-Datensätze aus 2 realen Fahrzeugen. Mit ihrer Erkennung erreichen Haga et al. eine False-Positive Rate (normale Nachricht wird fälschlicherweise als Anomalie eingestuft) von 0,0478% und eine False-Negative Rate (Anomalie wird fälschlicherweise als normal eingestuft) von 0,3288%.
In der Arbeit *Intrusion Detection by Density Estimation of Reception Cycle Periods for In-Vehicle Networks: A Proposal* von Hamada et al. [15] wird die Erkennung von Anomalien bei periodischen CAN-Nachrichten im Fahrzeug-Netzwerk durch eine statistische Analyse mit Hilfe von Standardverfahren (hier: Maximum Likelyhood Estimation, 2nd Mixture Gaussian Distribution Model) behandelt. Konkret wurden die Varianzen der Perioden der zyklischen Nachrichten analysiert, um Anomalien zu erkennen. Diese IDS-Lösung ist ausreichend effizient, sodass keine Auslagerung von Funktionalität auf externe leistungsstärkere Server notwendig ist, beschränkt sich allerdings ausschließlich auf zyklische Daten. Mit ihrer Erkennung erreichen Hamada et al. eine False-Positive Rate von 1,23% und eine False-Negative Rate von 1,15%. Sowohl die Arbeit [14], als auch [15] befasst sich mit der Erkennung von Anomalien in der Fahrzeug-internen Kommunikation. Dabei werden konkrete Algorithmen für die Erkennung untersucht. Auch eine Auslagerung von Funktionalität für die Anomalie-Erkennung aus dem Fahrzeug in externe Server aus Performance-Gründen wird thematisiert, worauf auch in dieser Arbeit eingegangen wird. Im Gegensatz zu den eben vorgestellten Arbeiten [14] und [15] befasst sich diese Arbeit mit der Absicherung der externen Fahrzeug-Kommunikation. Dafür wird ein Architektur-Entwurf für ein Automotive Security-Gateway mit IDS entwickelt. Konkrete Algorithmen zur Anomalie-Erkennung werden hier nicht vorgestellt. Außerdem geht diese Arbeit von einem moderneren Fahrzeug-Netzwerk aus, in dem Real-Time Ethernet den CAN-Bus als zentrales Kommunikationsmedium abgelöst hat.
In der Arbeit *Sichere Anbindung von lokalen Netzen an das Internet* des BSI [6] werden Grundlagen der klassischen IT-Security, u.a. auch das Konzept des Security-Gateways, behandelt. In dem für diese Arbeit relevanten Teil von [6] wird die allgemeine Architektur eines Security-Gateways vorgestellt. Das Security-Gateway besteht aus 3 in Reihe geschalteten Filter-Komponenten (Siehe: Abbildung 5). Die erste ist ein Paketfilter für eingehende Daten, die zweite ein so genanntes Application-Level-Gateway (ALG) und die dritte ein Paketfilter für ausgehende Daten. Man spricht von einer dreistufigen PAP-Struktur (Paketfilter - Application-Level-Gateway - Paketfilter). Paketfilter verhindern Angriffe auf der Internet- und Transport-Schicht. Der Datenverkehr

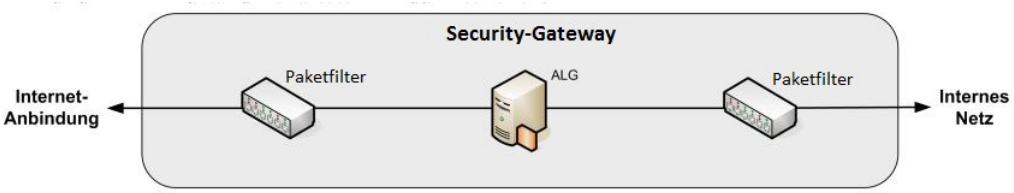

Abbildung 5: Architektur eines Security-Gateways (Quelle: [6], S.54 (abgeändert))

wird anhand spezieller Regeln gefiltert. Paketfilter können sowohl stateless als auch stateful sein. Ein ALG überwacht und kontrolliert die Kommunikation auf der Anwendungsschicht. Außerdem

dient es den Diensten im zu schützenden Netzwerk als Proxy und leitet ein- und ausgehende Anfragen entsprechend weiter. Bei verschlüsselter Kommunikation muss das ALG die Daten ent- und wieder verschlüsseln. Um seine Aufgaben mit ausreichend geringer Latenz zu erfüllen, muss ein ALG entsprechend leistungsstark sein. Ergänzend zu [6] wird in der Arbeit *Next Generation Firewalls* des BSI [7] das Security-Gateway um eine Next Generation Firewall (NGFW) Komponente erweitert. Eine NGFW enthält einen Stateful-Inspection Paketfilter und untersucht außerdem die Daten auf der Anwendungsschicht. Zur Untersuchung verschlüsselter Daten bietet sie die nötige Ver- und Entschlüsselungs-Funktionalität. Zusätzlich enthält eine NGFW (u.a.) ein IDS. Im Gegensatz zum ALG nimmt die NGFW nicht die Rolle eines Proxys ein, sondern leitet die Daten direkt weiter (Forwarding). Die NGFW ersetzt den Paketfilter hinter dem Application-Level-Gateway in der PAP-Struktur. Die Aufgaben des ALG und der NGFW überschneiden sich z.T. hinsichtlich der Überwachung des Datenverkehrs auf Anwendungsschicht. Generell gibt es Szenarien in denen durch den Einsatz einer NGFW auf ein ALG verzichtet werden kann. Werden, wie in diesem Fall, sowohl das ALG, als auch die NGFW in einer PAP-Struktur verwendet, wird die NGFW als höherwertiger Paketfilter (mit IDS) in dieser Struktur betrieben, während das ALG den Großteil der Arbeit auf Anwendungsschicht übernimmt. Für die in dieser Arbeit entwickelte Architektur eines Security-Gateways für den Automotive-Bereich wird der Ansatz des BSI aufgrund der ähnlichen Anforderungen an das Security-Gateway als Grundlage übernommen. Im Gegensatz zu den Arbeiten des BSI ist diese Arbeit im Automotive-Kontext angesiedelt und geht außerdem detailliert auf die IDS-Komponente des Gateways ein.

In ihrer Arbeit [25] stellen Pese et al. ihr Konzept einer Firewall zur Absicherung der Fahrzeuginternen Inter-Domain-Kommunikation vor. Konkret wird von einer Domain Architektur im Fahrzeug ausgegangen und die Firewall soll Angriffe aus einer Domain heraus auf Devices in einer anderen Domain verhindern (Siehe: Abbildung 6). In diesem Fall beschränkt sich der Begriff "Firewall" auf einen Paketfilter. Als Anforderungen an eine Firewall im Automotive Bereich generell werden Echtzeitfähigkeit, hoher Durchsatz und geringer Speicher- und CPU-Verbrauch genannt. Für den geringen Speicher- und CPU-Verbrauch werden Kostengründe aufgeführt. Es soll eine optimale Aufteilung der Firewall in Hardware- und Software-Komponenten erreicht werden. Die Firewall besteht aus einem einfachen stateless Paketfilter, welcher in Hardware (FPGA) realisiert wurde und einem stateful Paketfilter, welcher in Software realisiert wurde. Der stateless Paketfilter untersucht nur den Header eines Pakets und filtert anhand einer vordefinierten Whitelist. Der stateful Paketfilter untersucht die Daten auf der Transportschicht (nur TCP) und verhindert so z.B. SYN-Flooding Angriffe. Die entwickelte Firewall wurde in einer realen Umgebung hinsichtlich Durchsatz, Latenz und Speicher- und CPU-Verbrauch evaluiert. Die in [25] abgeleiteten Anforderungen an eine Automotive-Firewall ähneln den in dieser Arbeit abgeleiteten Anforderungen an ein Automotive Security-Gateway. Für die Absicherung der Fahrzeug-internen Kommunikation sind die Echtzeitanforderungen allerdings deutlich härter als bei der externen Fahrzeug-Kommunikation. Die Automotive Firewall von [25] beschränkt sich auf einen Paketfilter mit Stateful Packet Inspection. In dieser Arbeit hingegen wird die Architektur eines Security-Gateways behandelt, welches mehr Funktionalität, wie z.B. ein IDS, bietet.

Die Arbeit von Bouard et al. [2] behandelt die Absicherung der Kommunikation zwischen CE-Devices (Consumer Electronics) und ECUs im Fahrzeug durch eine Proxy-Komponente. Die Anforderungen an ein solches System, welches die Integration von CE-Devices erlaubt, sind, neben der kryptographischen Sicherheit, die Skalierbarkeit und eine ausreichende Trennung von den Fahrzeug-internen Diensten, sodass deren korrekte Ausführung in jedem Fall gewährleistet ist. Die Proxy-Komponente sorgt für eine lose Kopplung zwischen externen Devices und den ECUs im Fahrzeug-Netzwerk. Sie leitet Nachrichten von den CE-Devices an die ECUs weiter und umgekehrt. Die Proxy-Komponente kommuniziert über eine sichere IP-basierte Middleware, wie z.B. SEIS [11], mit den ECUs. Für eingehende Nachrichten wird die Authentizität des Senders überprüft. Nachrichten von nicht authentifizierten CE-Devices werden nicht an die entsprechende ECU weitergeleitet. Die in [2] beschriebene Komponente für die sichere Integration von CE-Devices überprüft die Authentizität externer Kommunikationspartner und erfüllt eine Proxy-Funktion, womit sie Teilfunktionalität eines Security-Gateways bietet. Diese Arbeit behandelt die Architektur eines solchen Security-Gateways, welches darüber hinaus Funktionalität, wie z.B. ein IDS, bietet und sich nicht auf CE-Devices beschränkt, sondern die komplette Kommunikation mit der Außenwelt absichert (Siehe: Abbildung 6).

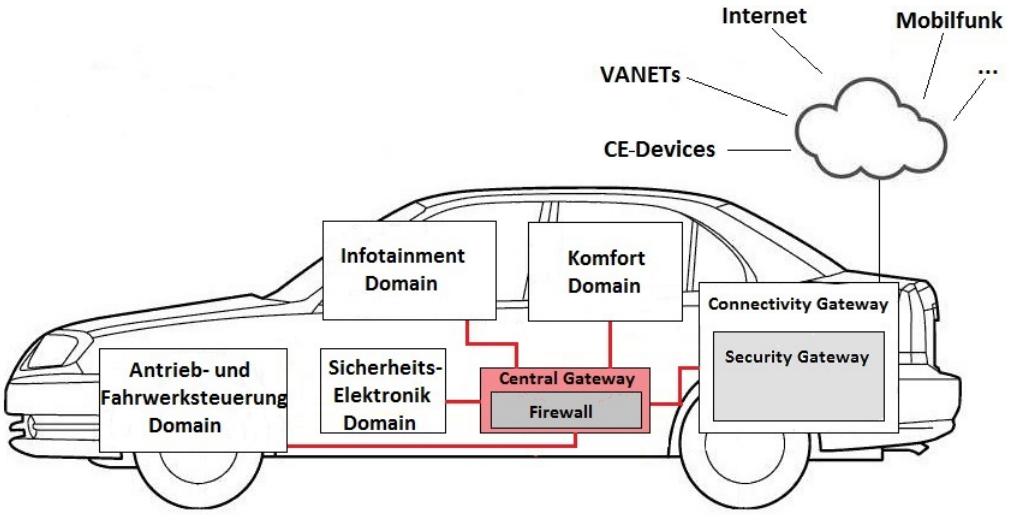

Abbildung 6: Schematische Abbildung: Fahrzeug mit Security-Gateway

4 Security Gateway

In diesem Abschnitt werden die Anforderungen an ein Security-Gateway im Automobil und eine daraus abgeleitete Architektur vorgestellt.

4.1 Anforderungen an ein Security-Gateway im Automobil

In der klassischen IT-Security sind Security-Gateways bereits lange etabliert. Inwieweit sich der Ansatz des Security-Gateways aus der klassischen IT-Security in den Automotive-Bereich übertragen lässt, wird im Folgenden untersucht. Dazu werden zuerst die Anforderungen an ein Security-Gateway der klassischen IT-Security aufgelistet. Diese werden in Performance- und funktionale Anforderungen aufgeteilt. Die Performance-Anforderungen sind ein hoher Datendurchsatz und eine geringe Latenz [6] [25]. Zu den funktionalen Anforderungen zählen:

- die Paketfilterung nach festgelegten Regeln,
- die Kontrolle der Daten auf der Anwendungsschicht (von der Protokollebene bis hin zu einer semantischen Analyse der Daten) und die damit einhergehende kryptographische Funktionalität,
- die Proxy-Funktion zwischen internen Diensten und der Außenwelt,
- ein IDS und
- die Konfigurierbarkeit des Systems (Filterregeln, IDS-Konfiguration) [6] [7].

Diese Anforderungen gelten auch im Automotive-Bereich, wobei hier zusätzlich die folgenden Punkte zu beachten sind:

- Die sichere Aufbewahrung kryptografischer Schlüssel im Fahrzeug ist schwieriger als in der klassischen IT-Security, da Angreifer u.U. direkten physischen Zugang zum Fahrzeug haben.
- Auch die Konfiguration des Systems im Fahrzeug ist schwieriger als in der klassischen IT-Security. Für eine praktikable Konfigurierbarkeit des Systems ist die Möglichkeit sicherer ECU-Updates eine Voraussetzung, da aufgrund des sehr langen Product-Life-Cycles beim Fahrzeug [25] mehrere Konfigurationen nötig sein werden.

Zusätzlich zu den aus der klassischen IT-Security bekannten Anforderungen kommen folgende Performance- und funktionale Anforderungen, die sich aus dem Automotive-Kontext ergeben:

- Wie in Abschnitt 2.2.2 beschrieben, ergeben sich aus der Service-Domain "Antrieb- und Fahrwerksteuerung" der externen Fahrzeug-Kommunikation harte Echtzeit-Anforderungen. Für V2V-Anwendungen wie Kollisionsvermeidung liegen die Echtzeit-Anforderungen bspw. im Millisekunden-Bereich [29].
- Außerdem wird aus Kostengründen ein möglichst geringer Speicher- und CPU-Verbrauch für das Security-Gateway gefordert [25].
- Zu den funktionalen Anforderungen zählt die Unterstützung verschiedener, mit unterschiedlichen Technologien (WLAN/Wi-Fi (IEEE 802.11), Bluetooth, UMTS, LTE und zukünftig 5G) transportierter Protokolle. Neben IP-basierten Protokollen sind hauptsächlich noch Protokolle zur V2V-, bzw. V2I-Kommunikation relevant. Hinsichtlich der Protokolle liegt der Fokus dieser Arbeit auf den IP-basierten Protokollen.
- Außerdem ist eine ausreichende Trennung des Security-Gateways von den Fahrzeug-internen Diensten nötig, sodass deren korrekte Ausführung auch bei Fehlfunktionen oder einem Ausfall des Security-Gateways in jedem Fall gewährleistet ist [2].

Abschließend werden an dieser Stelle alle Anforderungen an ein Automotive Security-Gateway aufgelistet:

Performance-Anforderungen	**Funktionale Anforderungen**
1) hoher Datendurchsatz	1) Paketfilterung nach festgelegten Regeln
2) Echtzeit-Fähigkeit	2) Kontrolle der Daten auf der Anwendungsschicht
	3) kryptographische Funktionalität
	4) Proxy-Funktion zwischen Fahrzeug-internen Diensten und Außenwelt
	5) IDS
	6) Konfigurierbarkeit
	7) Unterstützung IP-basierter und nicht IP-basierter Protokolle
	8) ausreichende Trennung von den Fahrzeug-internen Diensten

Tabelle 2: Anforderungen an ein Automotive Security-Gateway

4.2 Security-Gateway Architektur

Das Security-Gateway ist ein wichtiger Teil des Connectivity-Gateways. Seine Aufgabe ist die Absicherung der externen Fahrzeug-Kommunikation. Da sich die Anforderungen an das Automotive Security-Gateway, die in Abschnitt 4.1 definiert wurden, zu einem großen Teil mit denen aus der klassischen IT-Security überdecken und der wesentliche Unterschied in der Echtzeitfähigkeit und der größeren Anzahl an unterstützten Protokollen - nämlich zusätzlich auch nicht IP-basierten Protokollen - liegt, wurde für die grundlegende Architektur der in Abschnitt 3 beschriebene Ansatz aus der klassischen IT-Security übernommen. Dem Automotive Security-Gateway liegt eine dreistufige PAP-Struktur (Paketfilter - Application-Level-Gateway - Paketfilter) zugrunde (Siehe: Abbildung 7). Die 3 in Reihe geschalteten Komponenten sind für den gesamten IP-basierten Datenverkehr zuständig. Die erste Komponente ist ein Stateful-Inspection Paketfilter zum Verhindern von Angriffen auf der Internet- und Transport-Schicht, wie z.B. dem TCP SYN-Flooding. Damit wird die funktionale Anforderung 1 (aus Abschnitt 4.1) erfüllt. Bei der zweiten Komponente handelt es sich um ein Application-Level-Gateway (ALG) welches die Kommunikation auf der Anwendungsschicht kontrolliert, bspw. durch eine semantische Analyse der Daten, wodurch z.B. das unbefugte Versenden von vertraulichen Daten aus dem Fahrzeug verhindert werden kann. Es dient den Fahrzeug-internen Diensten als Proxy zur Außenwelt und leitet ein- und ausgehende Anfragen entsprechend weiter. Bei verschlüsselter Kommunikation muss das ALG die Daten ent- und wieder verschlüsseln. Mit dem ALG werden also die funktionalen Anforderungen 2, 3 und 4 erfüllt. Die dritte Komponente ist eine Next Generation Firewall. Diese enthält neben einem Stateful-Inspection Paketfilter für ausgehende Daten ein IDS (Siehe: Abschnitt 4.3) zur Untersuchung des Datenverkehrs, bspw. auf Anomalien wie z.B. deutlich erhöhte Paketrate oder veränderte Paketgröße. Damit wird die funktionale Anforderung 5 erfüllt.
Für nicht IP-basierten Datenverkehr, z.B. echtzeit-kritische V2V-Kommunikation, wird eine weitere PAP-Struktur parallel zu den Komponenten für IP-basierten Datenverkehr vorgeschlagen (Siehe: Abbildung 7), womit auch die funktionale Anforderung 7 erfüllt wird. Diese ist funktional auf nicht IP-basierten Datenverkehr zugeschnitten. Durch diese Aufteilung wird echtzeit-kritischer nicht IP-basierter Datenverkehr, z.B. V2V-Kommunikation, im Security-Gateway nicht durch die Überprüfung des IP-basierten Datenverkehrs zusätzlich verzögert und somit Performance-Anforderung 2 erfüllt. Die Anforderung eines hohen Datendurchsatzes (Performance-Anforderung 1) kann grund-

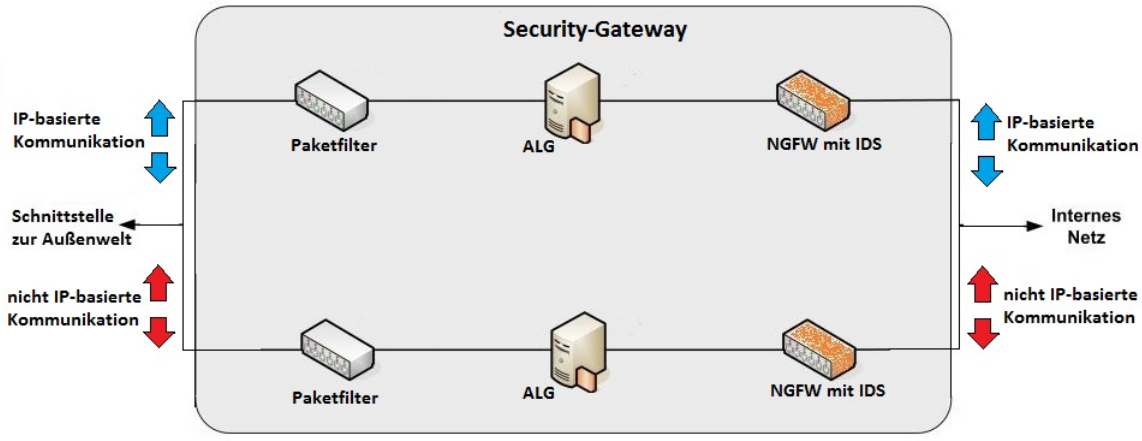

Abbildung 7: Automotive Security Gateway Architektur (Quelle: [6], S.54 (abgeändert))

sätzlich erfüllt werden, da die Architektur keine Struktur-bedingten Bottlenecks aufweist. Auch die Konfigurierbarkeit (funktionale Anforderung 6) ist unter Voraussetzung sicherer Software-Updates grundsätzlich gegeben. Eine ausreichende Trennung des Security Gateways von den Fahrzeug-internen Diensten (funktionale Anforderung 8), damit deren korrekte Ausführung auch bei Fehlfunktionen oder einem Ausfall des Security-Gateways in jedem Fall gewährleistet ist, kann generell durch eine lose Kopplung, z.B. durch den Einsatz einer Middleware, erreicht werden. Damit erfüllt die hier entwickelte Architektur alle in Abschnitt 4.1 definierten Anforderungen.

4.3 Intrusion Detection System Architektur

Dieser Abschnitt stellt die Architektur eines IDS für den Einsatz in einem Automotive Security-Gateway vor. Ein IDS besteht generell aus den folgenden Komponenten: 1) einem oder mehreren Sensoren (”Detection”), 2) einer Auswertungs-Station (”Decision”), 3) Datenbank-Komponenten und 4) einer Management-Station (Siehe: Abbildung 8) [5]. Die Sensoren sind zuständig für die Überwachung des Datenverkehrs und die Erkennung von Anomalien bei ”Anomaly-based IDS”, bzw. Abweichungen von der Spezifikation bei ”Specification-based IDS”. Auf eine solche Erkennung folgt die Benachrichtigung der Auswertungs-Station. Die Auswertungs-Station ist für die Analyse der Meldungen von den Sensoren (z.B. Klassifikation), die Reaktion auf diese und die Ablage dieser Meldungen für eine weitere Verwendung zuständig. Für die Speicherung der anfallenden Daten von der Auswertungs-Station sind die Datenbank-Komponenten vorhanden. Außerdem enthalten sie sämtliche Modelle und Regeln mit denen die Sensoren und die Auswertungs-Station arbeiten. Diese Modelle und Regeln müssen nicht immer von Experten erstellt werden, sondern können auch mit Machine Learning aufgrund von Trainingsdaten erlernt werden [23]. Das Lernen und Erstellen der Modelle und Regeln findet dann wegen den benötigten Ressourcen nicht auf dem Zielsystem mit dem IDS statt, sondern auf einem leistungsstarken Server. Eine sichere Datenübertragung vom Server auf das Zielsystem muss in einem solchen Fall natürlich gewährleistet sein. Die Management-Station ist für die Konfiguration, Kalibrierung und Überwachung der restlichen Komponenten des IDS zuständig.

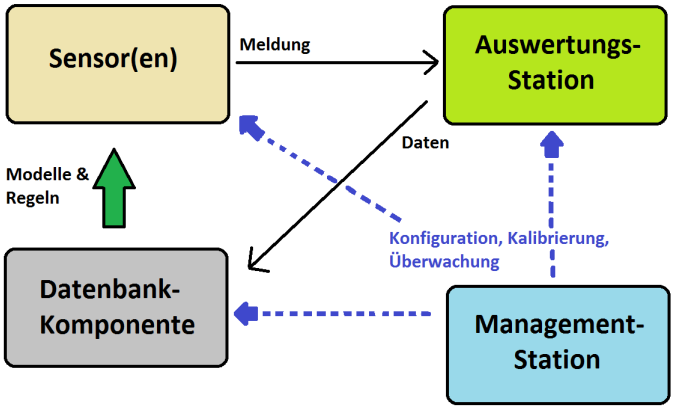

Abbildung 8: Schematische Darstellung: IDS Komponenten

Ein modularer Aufbau der Sensor-Komponente(n) des IDS ermöglicht gute Skalierbarkeit und Wiederverwendbarkeit der einzelnen Module. Eine solche Architektur wird von [23] vorgestellt. Es gibt zwei Arten von Modulen für die Erkennung von Anomalien/Spezifikations-Verletzungen, welche mehrstufig abläuft: ”Base Detection Agents” und ”Meta Detection Agents” (Siehe Abbildung 9). ”Base Detection Agents” werden für die erste Stufe verwendet. Sie untersuchen den hereinkommenden Datenverkehr gemäß ihrer Konfiguration auf Abweichungen vom Normalzustand. So kann es bspw. einen ”Base Detection Agent” für die Untersuchung der Paketgröße geben, einen für die Paketrate usw. Die ”Base Detection Agents” leiten ihre Ergebnisse an einen ”Meta Detection Agent” weiter. Der ”Meta Detection Agent” untersucht diese Ergebnisse dann gemäß seiner Konfiguration und kann so, basierend auf den Ergebnissen mehrerer ”Base Detection Agents”, erkennen, ob eine Anomalie vorliegt. Ein solcher modularer und hierarchischer Aufbau erlaubt die Zusammenstellung einer Sensor-Komponente eines IDS für beliebige individuelle Anforderungen.
Für das Erstellen der Modelle und Regeln für die Erkennung und Auswertung sind bei [23] ”Remote Learning Agents” vorgesehen, welche mit entsprechenden Trainingsdaten versorgt werden müssen.

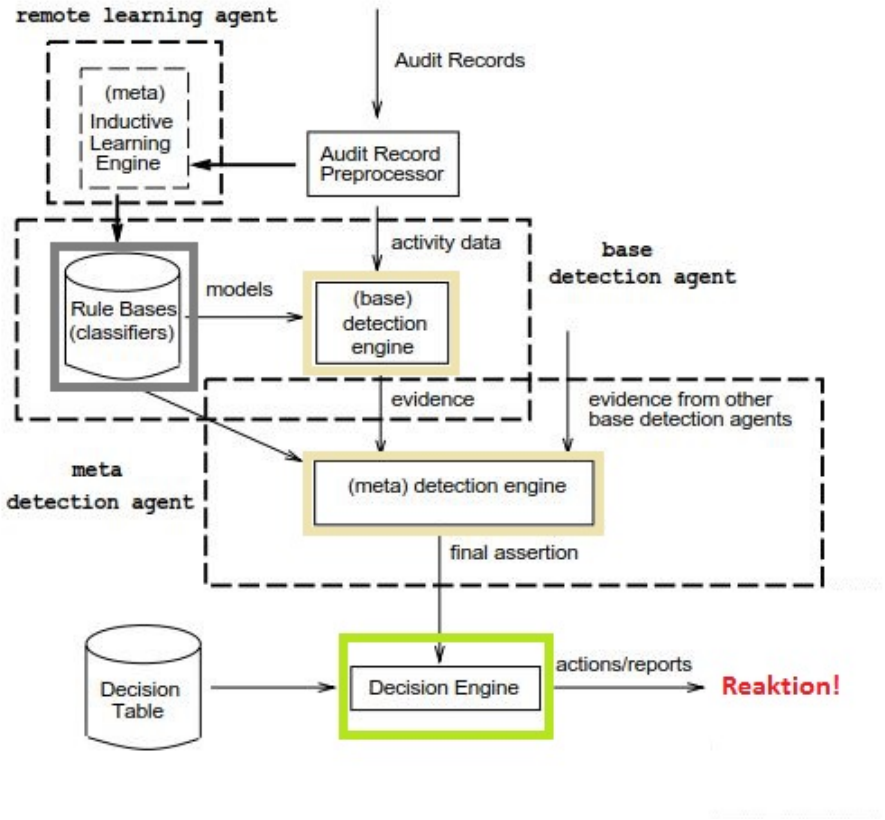

Abbildung 9: Architektur: Modulares IDS mit Learning Agents (Quelle: [23], S.14 (abgeändert))

5 Zusammenfassung und Ausblick

Zusammenfassung

In dieser Arbeit wurden die Anforderungen an ein Security-Gateway zur Absicherung der externen Fahrzeug-Kommunikation ermittelt und ausgehend davon eine Architektur für ein Security-Gateway im Automobil entwickelt. Die Anforderungen an ein solches Gateway lassen sich in Performance- und funktionale Anforderungen unterteilen. Die Performance-Anforderungen sind ein hoher Datendurchsatz und Echtzeitfähigkeit. Zu den funktionalen Anforderungen zählen die Paketfilterung nach festgelegten Regeln, die Kontrolle der Daten auf der Anwendungsschicht und die damit einhergehende kryptographische Funktionalität, die Proxy-Funktion zwischen Fahrzeug-internen Diensten und der Außenwelt, ein IDS, die Konfigurierbarkeit des Systems (Filterregeln, IDS-Konfiguration) und die Unterstützung verschiedener, mit unterschiedlichen Technologien (z.B. WLAN, Bluetooth, oder LTE) transportierter Protokolle. Neben IP-basierten Protokollen sind hauptsächlich noch Protokolle zur V2V-, bzw. V2I-Kommunikation relevant. Hinsichtlich der Protokolle liegt der Fokus dieser Arbeit auf den IP-basierten Protokollen. Da sich die Anforderungen an das Automotive Security-Gateway zu einem großen Teil mit denen aus der klassischen IT-Security überdecken und der wesentliche Unterschied in der Echtzeitfähigkeit und der größeren Anzahl an unterstützten Protokollen - nämlich zusätzlich auch nicht IP-basierten Protokollen - liegt, wurde für die grundlegende Architektur der Ansatz der klassischen IT-Security übernommen. Dem Automotive Security-Gateway liegt eine dreistufige PAP-Struktur (Paketfilter - Application-Level-Gateway - Paketfilter) zugrunde. Die 3 in Reihe geschalteten Komponenten sind für den gesamten IP-basierten Datenverkehr zuständig. Die erste Komponente ist ein Stateful-Inspection Paketfilter zum Verhindern von Angriffen auf der Internet- und Transport-Schicht. Bei der zweiten Komponente handelt es sich um ein Application-Level-Gateway (ALG) welches die Kommunikation auf der Anwendungsschicht kontrolliert. Es dient den Fahrzeug-internen Diensten als Proxy zur Außenwelt und leitet ein- und ausgehende Anfragen entsprechend weiter. Bei verschlüsselter Kommunikation muss das ALG die Daten ent- und wieder verschlüsseln. Die dritte Komponente ist eine Next Generation Firewall. Diese enthält neben einem Stateful-Inspection Paketfilter für ausgehende Da-

ten ein IDS zur Untersuchung des Datenverkehrs. Für das IDS des wurde dabei eine modulare Architektur gewählt, da sie eine gute Skalierbarkeit und die Wiederverwendbarkeit der einzelnen Module erlaubt. So können beliebige individuelle Anforderungen an die Erkennung erfüllt werden. Für nicht IP-basierten Datenverkehr, z.B. echtzeit-kritische V2V-Kommunikation, wird eine weitere PAP-Struktur parallel zu den Komponenten für IP-basierten Datenverkehr vorgeschlagen. Diese ist funktional auf nicht IP-basierten Datenverkehr zugeschnitten. Durch diese Aufteilung wird echtzeit-kritischer nicht IP-basierter Datenverkehr, z.B. V2v-Kommunikation, im Security-Gateway nicht durch die Überprüfung des IP-basierten Datenverkehrs zusätzlich verzögert.

Ausblick

Das Ziel zukünftiger Arbeiten ist die Entwicklung eines Prototypen des Automotive Security-Gateways in Hardware. Nachdem mit dieser Arbeit eine Architektur für ein solches Gateway entwickelt wurde, ist der nächste Schritt eine Realisierung der zentralen Komponente des Automotive Security-Gateways: des Application-Level-Gateways. In Zukunft könnte die Next Generation Firewall Komponente, welche ein IDS enthält, entwickelt werden. Dazu müssen konkrete Modelle und Regeln zur Untersuchung des externen Fahrzeug-Datenverkehrs erstellt werden. Zur Evaluierung des Automotive Security-Gateways oder einzelner entwickelter Komponenten hinsichtlich Performance und grundlegender Funktionalität könnten Simulationen in OMNeT++ durchgeführt werden. Auch eine Untersuchung der sicheren Speicherung und Verwaltung kryptographischer Schlüssel in Automotive-Hardware oder eine Weiterführung der Diskussion über die Verteilung kryptographischer Funktionalität zwischen dem Security-Gateway und den unterschiedlichen ECUs wären mögliche zukünftige Themen.

Literatur

[1] APVRILLE, Ludovic, et al.: Secure automotive on-board electronics network architecture. In: FISITA 2010 world automotive congress, Budapest, Hungary. 2010.

[2] BOUARD, Alexandre, et al. Automotive proxy-based security architecture for ce device integration. In: International Conference on Mobile Wireless Middleware, Operating Systems, and Applications. Springer, Berlin, Heidelberg, 2012. S. 62-76.

[3] BROY, Manfred; KRUGER, Ingolf H.; PRETSCHNER, Alexander; SALZMANN, Christian: Engineering Automotive Software. In: PROCEEDINGS-IEEE 95 (2007), Nr. 2, S. 356. – URL: https://mediatum.ub.tum.de/doc/1251761/1251761.pdf. Zugegriffen: 28.04.2018

[4] BROY, Manfred: Model-Driven Development of Reliable Automotive Services - Second Automotive Software Workshop, ASWSD 2006, San Diego, CA, USA, March 15-17, 2006, Revised Selected Papers, 2008th ed. Berlin Heidelberg: Springer Science Business Media, 2008.

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI); ConSecur GmbH: Einführung von Intrusion-Detection-Systemen - Grundlagen, 31. Oktober 2002, Version 1.0

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI): Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA), BSI-Standards zur Internet-Sicherheit (ISi-S), Version 2.1 vom 26.08.2014

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI): Next Generation Firewalls, BSI-CS 112, Version 1.00 vom 07.04.2015

[8] DATTA, S. K. ; et al.: Integrating connected vehicles in Internet of Things ecosystems: Challenges and solutions. In: 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), June 2016, S. 1–6

[9] fortiss GmbH: The software car: Information and communication technology (ict) as an engine for the electromobility of the future / fortiss GmbH. mar 2011. – Forschungsbericht. summary of results of the ëCar ICT System Architecture for Electromobility"research project sponsored by the Federal Ministry of Economics and Technology

[10] FÜRST, S.; BECHTER, M.: AUTOSAR for Connected and Autonomous Vehicles: The AUTOSAR Adaptive Platform. In: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), June 2016, S. 215–217

[11] GLASS, Michael, et al.: Seis—security in embedded IP-based systems. ATZelektronik worldwide, 2010, 5. Jg., Nr. 1, S. 36-40.

[12] HÄCKEL, Timo: Schnittstellen und Interaktionen zwischen fahrer- und fahrzeugbezogenen Diensten. Hochschule für Angewandte Wissenschaften Hamburg (2016)

[13] HÄCKEL, Timo: Service Classification in Service-Oriented ICT Architectures of Future Vehicles. Hochschule für Angewandte Wissenschaften Hamburg (2017)

[14] HAGA, Tomoyuki; et al.: Automotive SIEM and Anomaly Detection Using Sand-Sprinkled Isolation Forest, 15th Escar Europe Conference, Berlin, November 2017

[15] HAMADA, Y.; et al.: Intrusion detection by density estimation of reception cycle periods for in-vehicle networks: A proposal. In: 14th Int. Conf. on Embedded Security in Cars (ESCAR 2016), Munich, Germany. 2016.

[16] HOPPE, Tobias; KILTZ, Stefan; DITTMANN, Jana: Applying intrusion detection to automotive it-early insights and remaining challenges. Journal of Information Assurance and Security (JIAS), 2009, 4. Jg., Nr. 6, S. 226-235.

[17] IAV: Homepage - Sicherheitselektronik
https://www.iav.com/engineering/fahrzeugsicherheit/sicherheitselektronik
Zugegriffen: 29.04.2018

[18] IDREES, Sabir; et al. Secure automotive On-Board protocols: A case of over-the-air (OTA) firmware updates, Nets4Cars-2011 3rd International Workshop on Communication Technologies for Vehicles (Nets4Cars-2011)(Oberpfaffenhofen-Wessling, Munich, Germany), 3 2011. Cited on, S. 64.

[19] IWAI, Akihito; AOYAMA, Mikio: Automotive cloud service systems based on service-oriented architecture and its evaluation. In: Cloud Computing (CLOUD), 2011 IEEE International Conference on. IEEE, 2011. S. 638-645.

[20] JOBST, Martin Erich; PREHOFER, Christian: Towards hierarchical information architectures in automotive systems. In: Emerging Ideas and Trends in Engineering of Cyber-Physical Systems (EITEC), 2016 3rd International Workshop on. IEEE, 2016. S. 41-46.

[21] JONES, Andrew Michael: Architecting Secure Automotive Systems - Arm technology for next generation vehicular microcontrollers, Architecture and Technology Group, Arm, Oktober 2017

[22] KLEBERGER, Pierre; OLOVSSON, Tomas; JONSSON, Erland: Security aspects of the in-vehicle network in the connected car. In: Intelligent Vehicles Symposium (IV), 2011 IEEE. IEEE, 2011. S. 528-533.

[23] LEE, Wenke; STOLFO, Salvatore J.: Data Mining Approaches for Intrusion Detection, Proceedings of the 7th USENIX Security Symposium San Antonio, Texas, January 26-29, 1998

[24] MÜLLER, Klaus-Rainer: IT-Sicherheit mit System: integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement - sichere Anwendungen - Standards und Practices, S. 439 (2014)

[25] PESÉ, Mert D.; SCHMIDT, Karsten; ZWECK, Harald. Hardware/Software Co-Design of an Automotive Embedded Firewall. SAE Technical Paper, 2017.

[26] PRETSCHNER, Alexander; BROY, Manfred; KRUGER, Ingolf H.; STAUNER, Thomas: Software Engineering for Automotive Systems: A Roadmap. In: 2007 Future of Software Engineering. Washington, DC, USA : IEEE Computer Society, 2007 (FOSE '07), S. 55–71. – URL: http://dx.doi.org/10.1109/FOSE.2007.22. Zugegriffen: 28.04.2018 ISBN 978-0-7695-2829-8

[27] SCHUNTER, Matthias; et al.: Vehicle to Cloud - Research Challenges for Intelligent Vehicles, 15th Escar Europe Conference, Berlin, November 2017

[28] VAN ROERMUND, Timo; et al.: Securing the In-Vehicle Network of the Connected Car, 14th Escar Europe Conference, München 2016

[29] YANG, Xue, et al. A vehicle-to-vehicle communication protocol for cooperative collision warning. In: Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004. The First Annual International Conference on. IEEE, 2004. S. 114-123.