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

Andre Bücker
T-Systems GEI GmbH
andre.buecker@t-systems.com

Christian Bernhold
T-Systems International GmbH
christian.bernhold@t-systems.com

Entwicklung eines autarken Intrusion Detection Systems (IDS) mit fahrzeugbasierten Crowd-Ansatz

Zusammenfassung

Aktuelle Fahrzeugnetzwerke (CAN, MOST, LIN, FlexRay, Ethernet, etc.) bildeten bisher ein durch die Fahrzeugabmessungen begrenztes eigenständiges Ökosystem. Mit der zunehmenden Vernetzung von Fahrzeugen ändert sich dies seit geraumer Zeit. Fahrzeuge werden immer mehr zu digitalen Kommunikationsobjekten, die ihre Daten mit Backendsystemen oder anderen Fahrzeugen austauschen.
Viele Unternehmen in der Automobilindustrie sehen sich zunehmend Gefahren ausgesetzt, die bisher aus der Welt der globalen IP Vernetzung bekannt waren, der Gefahr von Hackerangriffen. Die zunehmende Vernetzung von Fahrzeugen durch

- Einführung mobiler Online Dienste
- Einführung von kostenpflichtigen Funktionalitäten und Services
- Gesetzmäßig vorgeschriebene Einführung des emergency calls (eCall)
- Vorbereitung der Schnittstellen in Richtung des autonomen Fahrens

führt dazu, dass die Fahrzeuge in immer stärkerem Maße mit ihrer Umgebung kommunizieren. Diese neu geschaffenen Schnittstellen können im Falle vorhandener Schwachstellen von Angreifern ausgenutzt werden, so dass Fahrzeugfunktionen im Sinne des Angreifers manipuliert werden können.
Während HTTP bzw. HTTPS Verbindungen über die Luftschnittstelle relativ gut über etablierte Verfahren abgesichert werden können, findet man im Netzwerkverkehr im Fahrzeug, historisch bedingt, kaum derartige Sicherheitskonzepte. Diese Schachstellen wurden von OEMs und Tier1s bereits identifiziert, deshalb versucht man aktuell auch innerhalb des bestehenden Fahrzeugnetzwerkes Verschlüsselungstechnologien einzusetzen. Diese setzen sich allerdings noch zögerlich durch und führen ohnehin nur dazu, dass sich das Problem von Cyberangriffen auf eine höhere Komplexitätsstufe verschiebt, das grundsätzliche Problem bleibt nach wie vor bestehen.

1. Die Lösung

Ein System, mit dem Fahrzeugnetzwerke auf Anomalien untersucht und mittels moderner Machine Learning Methoden sukzessive auf dem aktuellen Sicherheitsstand gehalten werden (Intrusion Detection System - IDS). Das Feststellen bekannten Fehlverhaltens, löst ein zuvor mit dem Fahrzeughersteller abgestim-

doi: 10.15771/ASW_2017_2

mtes Abwehrverhalten des Fahrzeugs aus (Intrusion Prevention System - IPS), damit ein Hackerangriff auf das interne Fahrzeugnetzwerk im Idealfall keinen negativen Einfluss auf die Fahrzeugfunktionen und damit auf die Sicherheit der Fahrzeuginsassen hat.
Die prinzipielle Funktionsweise wird durch folgende Darstellung erkennbar.

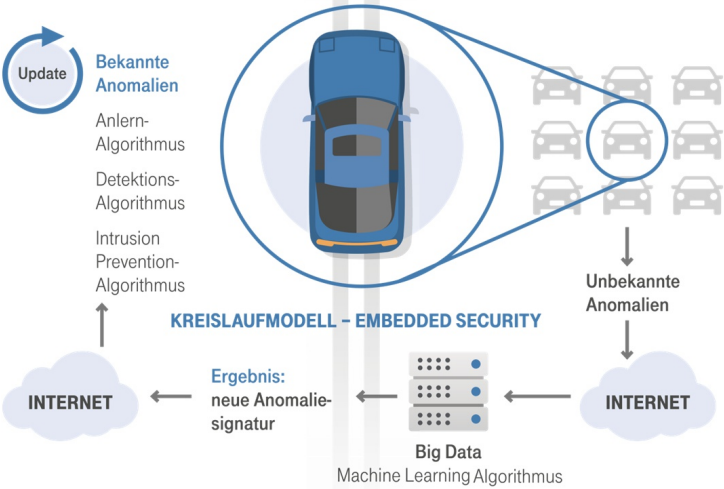

Abbildung 1: Funktionsprinzip

Eine AUTOSAR-konforme onboard-SW gleicht dynamisch das SOLL-Verhalten ab. Entspricht der aktuelle Netzwerkverkehr nicht dem definierten Verhalten, so findet im nächsten Schritt eine Klassifizierung des aktuellen Netzwerkverkehrs in „bekannte Anomalie“ (bekanntes Fehlverhalten) oder „unbekannte Anomalie“ (unbekanntes Verhalten) statt.
Eine AUTOSAR-konforme onboard-SW gleicht dynamisch das SOLL-Verhalten ab. Entspricht der aktuelle Netzwerkverkehr nicht dem definierten Verhalten, so findet im nächsten Schritt eine Klassifizierung des aktuellen Netzwerkverkehrs in „bekannte Anomalie“ (bekanntes Fehlverhalten) oder „unbekannte Anomalie“ (unbekanntes Verhalten) statt.
Die Anbindung des Fahrzeuges an ein zentrales Backendsystem ist für den fahrzeugbasierten Crowd – Ansatz von zentraler Bedeutung. Der ESLOCKS Service wird von den jeweiligen Fahrzeugen mit Informationen zu unbekannten Anomalien versorgt. Dabei wird gleichzeitig auch ein Netzwerk-Trace an den Service übermittelt, der sowohl eine definierte Periode vor dem Zeitpunkt der unbekannten Anomalie beinhaltet, als auch einen definierten Zeitraum danach. Über die Flotte der Fahrzeuge, die mit der entsprechenden onboard-SW ausgestattet sind, sammeln sich nach und nach im ELSOCKS Analyse Cluster große Men-

gen an Daten, diese werden performant in einem eigens eingerichteten Big Data Clusters abgelegt.
Die Auswertung erfolgt mittels verschiedener Machine Learning Methoden. Ziel der Massendatenauswertung ist es, unbekannte Anomalien entweder als Normalverkehr bzw. SOLL-Verhalten oder aber als Angriff bzw. neue bekannte Anomalie zu identifizieren. Die so gewonnenen Informationen werden aufbereitet und als Signaturupdate zurück in die Fahrzeuge übermittelt.
Die Signaturliste in den jeweiligen Fahrzeugen werden somit kontinuierlich mit neuen Erkenntnisse aus dem ESLOCKS Service aktualisiert. Hierdurch können die Fahrzeuge einerseits SOLL-Verhalten als solches erkennen und andererseits die Fahrzeuge gegen neu festgestellte Bedrohungsszenarien schützen. Dies stellt ein Kreislaufmodell dar, bei dem die onboard-SW mit ihrer größer werdenden Verbreitung in den Fahrzeugen und der damit einhergehenden größeren Datenbasis für die Massendatenauswertung fortlaufend optimiert wird.
Jede Signatur die vom ELOCKS Service an das Fahrzeug übermittelt wird, beinhaltet eine automotive Detektionsanweisung, dessen Deklaration mittels einer generischen Regelsyntax erfolgt, die im Rahmen dieser Lösung entwickelt wurde.

2. Übersicht der Features

Folgende Vorteile bietet die ESLOCKS Lösung:

- Selbstlernendes Intrusion Detection System (IDS)
- Verfahren setzt kein herstellerspezifisches Wissen voraus und damit allgemein einsetzbar
- Detektionsalgorithmus autark zu jeder Zeit, auch ohne Online-Verbindung zum ELOCKS Service, aktivAnomalien werden direkt im Fahrzeug erkannt
- Durch die AUTOSAR-konforme Entwicklung, ist die onboard-SW wiederverwendbar und leicht an verschiedene ECUs anpassbar
- Dynamische Interpretation von Signaturupdates zur Laufzeit, d.h. Verbesserung des Detektionsalgorithmus ohne Flashen des Steuergerätes auch während der Fahrt.
- Unbekannte Anomalien werden über die gesamte Flotte im ESLOCKS Service analysiert
- Modernste Machine Learning Algorithmen in der ESLOCKS Analyse erkennen auch komplexe Zusammenhänge
- Updatemechanismus sorgt für optimalen Schutz des Fahrzeugnetzwerkes durch Rückführung der Erkenntnisse aus dem ELOCKS Service bei vorhandener online-Verbindung
- Verwendung einer generischen Regelsyntax zur Deklaration von Signaturen bzw. automotiven Fahrzeug Bus Detektionsanweisungen.
- Personenbezogene Daten werden nicht erfasst, somit ist die Identität des Fahrers geschützt.
- Automatische Klassifizierung von Fahrzeuggruppen im ESLOCKS Service
- Flottenbasierte Signaturaktualisierung auf Basis der Analyse einzelner Fahrzeug Anomalien (Crowd-Ansatz)
- Skalierbare und an OEM adaptierbare Lösung

3. Ausblick

Das ESLOCKS Verfahren ist nicht exklusiv auf den automotive Sektor beschränkt, sondern kann leicht auf andere Netzwerkverbunde wie Industrienetzwerke (Roboterfarmen, Industrie 4.0, IoT,…) ausgeweitet werden.
Um die Analysequalität weiter zu erhöhen, werden in den nächsten Ausbaustufen weitere Datenquellen, wie z.B. Umweltinformationen herangezogen, die einen erweiterten Einblick ermöglichen.