Technische Hochschule Ingolstadt

Seminar zu Themen der Informatik

Sommersemester 2021

Seminararbeit

WANNADRIVE?

Feasible Attack Paths and Effective Protection Against Ransomware in Modern Vehicles

von

Johannes Winter

1 Einleitung

In der Praxis hat sich jegliche Art von Cyber-Erpressungs-Malware auf IT-Systeme als sehr erfolgreich und lukrativ erwiesen. Jedes Jahr erzielen Erpresser so mehrere Milliarden US-Dollar Lösegeld und die Tendenz ist weiter steigend [1, vgl.]. Durch die zunehmende Vernetzung und Digitalisierung entstehen immer größere potenzielle Angriffsziele, welche Opfer eines Ransomware-Angriffs werden können. Der eigene Computer, Unternehmens-IT-Systeme, SmartHome-Geräte oder IoT-Geräte – alle sind der Gefahr ausgesetzt. Nur ein vernetztes Gerät, welches täglich von Milliarden von Menschen benutzt wird, ist bis zum jetzigen Standpunkt noch kein Opfer von Ransomware-Angriffen geworden – das Auto. Gerade im Automobilbereich spielt das Thema Vernetzung und Digitalisierung eine sehr große Rolle und man strebt das Ziel eines vollständig vernetzten Straßenverkehrs an. Ein Auto muss mittlerweile mehr können als nur fahren und besteht aus sehr vielen softwaregesteuerten Komponenten. Diese wiederum erhöhen somit auch die potenzielle Angriffsfläche, vor allem für Ransomware.
Der wissenschaftliche Artikel [2] befasst sich mit diesem Thema und diskutiert einen solchen Angriff sowohl in der Theorie als auch in der Praxis und stellt Präventiv- als auch Gegenmaßnahmen dar. Der Inhalt dieses Artikels wird im Folgenden zusammengefasst wiedergegeben.

2 Erfolgsrezept Ransomware?

Das Wort „Ransomware“ kommt von dem englischen Wort „ransom“ und bedeutet übersetzt „Lösegeld“. Dabei handelt es sich um Schadprogramme, meistens Erpressungssoftware oder Verschlüsselungstrojaner, mit denen ein Angreifer den Computer sperren und darauf befindliche Daten verschlüsseln kann. Erst nachdem das Opfer einer Lösegeldzahlung nachkommt, werden die Daten wieder freigegeben.
Im Gegensatz zu fahrzeugbezogenen IT-Systemen, wo zum heutigen Stand wenig relevante Ransomware-Angriffe bekannt sind, werden in anderen IT-Bereichen bereits erfolgreich Ransomware-Attacken durchgeführt. Egal ob öffentliche und private Unternehmens-IT-Systeme, industrielle Steuerungssoftware, Websites, Smartphones oder sogar Live-TV-Sender – jede Art von IT-Systemen kann und ist bereits Opfer eines Ransomware-Angriffs gewesen.

Aktuelle Studien schätzen den Anteil an infizierten, unaufgeforderten Emails auf bis zu 70%. Im Jahr 2016 haben so Cyberkriminelle bereits rund 1 Milliarde US-Dollar erpresst. 2021 wird der Umsatz auf bis zu 20 Milliarden US-Dollar ansteigen [1, vgl.].
Heutige Ransomware macht sich die zunehmende Digitalisierung und Konnektivität aller Lebensbereiche sowie die wachsenden Abhängigkeit von vernetzten IT-Systemen zunutze und genau dies könnte schon bald auch moderne Fahrzeuge betreffen. Fahrzeuge werden nämlich immer:

- Softwaregesteuerter (Vergrößerung der Anzahl potenzieller Angriffsziele)
- Vernetzter (Vergrößerung der potenziellen Angriffsfläche)
- Komplexer (Erhöhung der ausnutzbaren Sicherheitslücken),

was die Anfälligkeit gegenüber Cybersicherheitsangriffen deutlich erhöht.

In der Praxis wurden bereits alle bekannten Angriffsmuster hinsichtlich der Fahrzeugsicherheit (z.B. sicherheitskritische Fahrfunktionen wie Fahrzeuglenkung und -bremsung) erfolgreich demonstriert. Angriffe, welche sich jedoch auf die Fahrsicherheit des Fahrzeugs auswirken, noch nicht. Dies liegt daran, dass zur heutigen Zeit die häufigsten Fahrzeugsicherheitsangriffe immer noch dieselben sind wie früher: Fahrzeug-(Komponenten)Diebstahl, Kilometerzähler-Manipulation, (Chip-)Tuning und Herstellung gefälschter Teile.
Gegen Diebstahl oder Phishing (Ausnutzen unvorsichtigen Verhaltens) entwickelt die Automobilindustrie immer wieder neue und verschiedene Maßnahmen und Mechanismen. Ransomware hingegen wurde von den Sicherheitsingenieuren laut der Autoren noch nicht wirklich in Angriff genommen. Dafür sehen sie hauptsächlich zwei Gründe:

1. Die Erstellung eines Fahrsicherheitsangriffs erfordert viel Zeit und Geld (viele Personenarbeitsmonate & $>$100.000 Dollar Entwicklungskosten), ermöglicht aber nur einen Angriff auf einen bestimmten Fahrzeugtyp oder eine Fahrzeugklasse. Eine Übertragung ist aufgrund der Homogenität der meisten Fahrzeug-IT-Architekturen und Fahrzeug-IT-Softwaren nicht möglich.
2. Der finanzielle Gewinn bei einem solchen Angriff bleibt bisher noch aus und oftmals werden die Angreifer nur mit einer Anerkennung aus akademischen Kreisen belohnt.

Wie genau ein solcher Ransomware-Angriff in der Theorie und Praxis realisiert werden und aussehen könnte, wird in den nächsten Kapiteln beschrieben.

3 Fahrzeugbezogenen Ransomware in der Theorie

Da es nach aktuellem Stand noch keine öffentlich bekannten fahrzeugbezogenen Ransomware-Angriffe gibt, lassen sich die Voraussetzungen für solch eine Cyber-Attacke nur grob abschätzen und von anderen Ransomware-Angriffen im IT-Bereich übertragen. Damit jedoch ein derartiger Cyber-Angriff tatsächlich umgesetzt werden kann, bedarf es der Notwendigkeit mindestens folgender fünf Bedingungen:

1. Einen Ransomware-Malware-Client und eine Server-Software für die On-Board-Realisierung der Cyber-Erpressung auf dem Zielfahrzeug zusammen mit der entsprechenden Fernsteuerung
2. Ein anonymes Botnetz zur globalen Verteilung und Fernsteuerung der Ransomware-Fahrzeugclients
3. Ein fahrzeuginterner Sicherheits-Exploit, meist zusammen mit einer Trojaner-Software zum Erreichen und Infizieren einer angeschlossenen Fahrzeugeinheit, um den Ransomware-Malware-Client zu installieren und auszuführen
4. Eine bordeigene Sperr- oder Bricking-Aktion für eine kritische Fahrzeugkomponente, die nicht (leicht) wiederhergestellt oder umgangen werden kann oder die sich keine lange Ausfalldauer leisten kann - idealerweise kombiniert mit einem (geheimen) Entsperrbefehl, um die gesperrte Fahr-

zeugkomponente nach Zahlung des Lösegelds freizugeben

5. Ein anonymes Zahlungsschema zur Entgegennahme des Lösegelds und zum Schutz des Erpressers vor Enttarnung und anschließenden rechtlichen Schritten

Sind diese Voraussetzungen mindestens gegeben, dann könnte ein Ransomware-Angriff auf ein Fahrzeug wie folgt ablaufen:

Zu Beginn muss der Angreifer die Schadsoftware erstellen. Sobald eine funktionierende Ransomware programmiert wurde, muss diese auf die ausgewählten Erpressungs-Zielfahrzeuge mittels einer Ransomware-Steuerungssoftware verteilt werden. Im besten Fall geschieht dies mittels eines anonymen Botnetzes, welches beispielsweise auf der TOR-Technologie [1] basieren könnte.
Hat die Software das Zielfahrzeug erreicht, muss dieses infiziert werden. Das kann direkt oder indirekt erfolgen.
Eine direkte Infizierung könnte beispielsweise über eine USB-Schnittstelle oder Ladeschnittstelle realisiert werden. Eine indirekte Infizierung hingegen würde sich eine sekundäre Sicherheitslücke zu Nutze machen und über eine Zwischenkomponente versuchen, die Software auf das Fahrzeug zu laden. Das kann z.B. eine infizierte Website sein, auf welche das Fahrzeug zugreifet.
Wenn dieses Vorgehen erfolgreich ist und die Software das Fahrzeug erreicht hat, wird der integrierte primäre Sicherheits-Exploit des Fahrzeuges genutzt, um den Ransomware-Client auf einer zentralen, gut vernetzten Einheit im Fahrzeug zu installieren und auszuführen. Diese Einheit könnte z.B. das Infotainment-System sein, welche dann als Host für weitere Aktionen missbraucht wird.
Je nachdem, mit welchem Vorgehen die Erpresser das Auto manipulieren wollen, kann der Ransomware-Client entweder eine Online-Verbindung zurück zum Erpresser aufbauen, um weitere Daten und/oder Befehle zu erhalten oder den Weg direkt über die fahrzeuginternen Bussysteme nutzen. Über diese könnte die Schadsoftware mit kritischen Steuergeräten (z.B. Motorsteuerung) kommunizieren, um somit die geplante Sperraktion durchzuführen.
Ist dieses Vorhaben gelungen, muss nur noch die Erpressermeldung mit den nötigen Details zur anonymen Bezahlung auf einem Bildschirm im Fahrzeug angezeigt werden. Im Falle, dass das Opfer das geforderte Lösegeld tatsächlich bezahlt, würde die Ransomware erneut das Bot-Netzwerk kontaktieren, um den (geheimen) Entsperrbefehl zu erhalten, damit das Fahrzeug wieder freigeben werden kann.

4 Fahrzeugbezogenen Ransomware in der Praxis

In Kapitel 3 wurde erklärt, was eine fahrzeugbezogene Ransomware-Attacke für nötige Voraussetzungen haben muss und wie diese in der Theorie ablaufen könnten. In diesem Kapitel soll es nun darum gehen, wie dieses Vorhaben in der Praxis realisieren wären.
Dabei wird auf die Abläufe *„Erstellen einer fahrzeugbezogenen Ransomware-Malware“, „Verbreitung der Fahrzeug-Ransomware-Malware“, „Infizierung des Zielfahrzeugs“, „Erpressung im Zielfahrzeug“ und „Ablauf der Lösegeldzahlung und Freigabe des Zielfahrzeugs“* genauer eingegangen.

4.1 Erstellen einer fahrzeugbezogenen Ransomware

Wie bereits in Kapitel 2 erwähnt, ist fast jedes IT-System angreifbar für Ransomware und viele davon wurden bereits erfolgreich infiziert. Der dadurch entstandene lukrative Markt hat dazu geführt, dass es mittlerweile fertige Ransomware-Baukästen und Ransomware-as-a-Service (RaaS)-Angebote gibt. Solche Kits enthalten den notwendigen Malware-Kontrollserver und eine fertige Schnittstelle zu einem anonymen Bezahlungsmittel und Traffic-Anonymisierer.
Einige solcher Ransomware-Kits stellen darüber hinaus auch gängige Sicherheits-Exploits für die Ver-

[1] „The Onion Router“ – Verschlüsselung der Daten in mehreren Schichten, um anonymes surfen zu ermöglichen

teilung der Ransomware und Zielfunktion zur Verfügung. In manchen Fällen kann ein solches Kit sogar sogenannte „Zero-Day-Exploits“ zur Integration in die Software bereitstellen. Dabei handelt es sich um Sicherheitslücken, welche dem Entwickler bzw. Unternehmen der betroffenen Einheit noch nicht bekannt sind. Dadurch kann diese Schwachstelle noch individueller und leistungsfähiger ausgenutzt werden.
Selbst der gewünschte Erpressungsmechanismus kann bei solchen Baukästen ausgewählt werden. Egal ob Verschlüsseln der Daten, Sperren wichtiger Komponenten oder mögliches Freigeben sicherheitskritischer Daten – der Erpresser hat fast unbegrenzte Möglichkeiten, den für sich optimalen Erpressungsmechanismus auszuwählen.
So kann mittels dieser Kits ein Angreifer innerhalb kurzer Zeit und mit wenigen Klicks eine funktionierende Ransomware mit allen notwendigen Komponenten erstellen.
Bis jetzt ist es jedoch noch nicht möglich, mit Hilfe solcher Baukästen Schadsoftware für fahrzeugbezogene IT-Systeme zu erstellen, da die meisten Kits hauptsächlich für Microsoft Windows-Betriebssysteme ausgelegt sind. Laut Autoren ist es jedoch nur eine Frage der Zeit und finanziellen Attraktivität, bis solche Erstellungssoftwares auch für *Automotive Linux* oder *AUTOSAR-OS* programmiert werden.

4.2 Verbreitung der fahrzeugbezogenen Ransomware

Um die Ransomware auf eine große Anzahl an Fahrzeugen zu verbreiten und dabei sowohl effizient als auch anonym zu bleiben, bietet sich ein TOR-basiertes Botnetz an. Ein solches Botnetz kann in der nötigen Größe von mindestens 400.000 „Bot-Clients“ schon für 1000$ pro Woche angemietet werden.
Zwar erreichen solche Botnetze das Fahrzeug nicht direkt, können aber zumindest indirekt Fahrzeuge infizieren, indem sie ein Host-System befallen und missbrauchen, welches über einen digitalen Kommunikationskanal zum Fahrzeug verfügt. Solche Host-Systeme könnten sein:

- Websites, die vom Fahrzeug abgerufen werden (z. B. Drive-by-Downloads, die über die bordeigene Infotainment-Einheit oder über versteckte Machine-to-Machine-Website-Anfragen abgerufen werden)
- Nachrichten, die vom Fahrzeug abgerufen und interpretiert werden (z. B. E-Mails, SMS, digitale Messenger, E-Call, DAB+ Radio)
- Persönliche Geräte, die mit dem Fahrzeug verbunden sind (z. B. Smartphones, digitaler Speicher, Navigation, OBD-Plugins)
- Jedes mit dem Fahrzeug verbundene OEM- oder Lieferanten-Backend (z. B. für FOTA-Updates, Ferndiagnose, Cloud-Dienste)
- Jedes mit dem Fahrzeug verbundene Backend von Drittanbietern (z. B. für Versicherung, Telematik, Maut, Logistik, Leasing)
- Alle Geräte von Drittanbietern, die mit dem Fahrzeug verbunden sind (z. B. Anhänger, Fahrzeugperipherie oder Anbaugeräte, Elektroladestation, Werkstattgeräte, digitaler Fahrtenschreiber)
- Verkehrsinfrastrukturen (z. B. Verkehrsmanagementsysteme, Baustellenzugangskontrollgeräte, Mautsysteme, V2X)

Je nachdem, wie leistungsfähig die erstellte Ransomware ist, kann die Verbreitung der Schadsoftware entweder aktiv oder passiv erfolgen. Eine aktive Verbreitung ist möglich, wenn die Software eine gewisse Leistungsfähigkeit und einen sekundären Infektionsmechanismus besitzt. Ist die Leistungsfähigkeit jedoch nicht gegeben, dann muss die Verbreitung passiv erfolgen, d.h. über das entsprechende Botnetzwerk.

4.3 Infizierung des Zielfahrzeugs

Hat die Ransomware nun eine digitale Fahrzeugschnittstelle erreicht, muss der Client nur noch auf der entsprechend leistungsfähigen und gut vernetzten elektronischen Steuereinheit (ECU) im Fahrzeug installiert und ausgeführt werden.
Mehrere Studien bzw. Forschungsarbeiten haben bereits bewiesen, dass fahrzeuginterne Sicherheitslücken existieren, welche durch eine Ransomware missbraucht werden könnten. In einer dieser gelang es den Sicherheitsexperten Zugriff auf die interne Software zu erlangen. Von Ärgernissen wie unkontrolliertem Hupen bis hin zu ernsthaften Gefahren wie dem Bremsen des Prius bei hohen Geschwindigkeiten, dem Abschalten der Servolenkung, dem Fälschen des GPS und Tachometer wird berichtet. Mit den Befehlen, welche die ”Hacker”von ihren Laptops aus schickten, war fast alles möglich, um das Auto in eine gefährliche Fahrsituation zu bringen [3, vgl.].
Sowohl die zunehmende Digitalisierung, Vernetzung, Homogenisierung sowie Standardisierung im Fahrzeug tragen dazu bei, dass die Skalierbarkeit der Angriffe erhöht wird, da so mehr einheitliche Fahrzeugsicherheitsschwachstellen entstehen. Diese wären:

- Schwachstellen im USB-Anschluss des Fahrzeug-Infotainment-Systems
- Schwachstellen im OBD-Port für den Zugriff auf alle Busse im Fahrzeug
- CD/DVD-Player-Schwachstellen am Fahrzeug-Infotainment-System
- Bluetooth-Pufferüberlauf-Schwachstellen bei Fahrzeug-Infotainment-Einheit
- Zellulare Verwundbarkeit an der zentralen Fahrzeugkommunikationseinheit
- Wi-Fi-Schwachstellen am Ladesystem für Elektrofahrzeuge
- Remote-Schwachstellen am Telematik-Steuergerät (TCU) des Nachrüstmarktes
- Schwachstellen in mobilen Fahrzeug-Apps für den Zugriff auf Fahrzeuginterna
- Ausnutzung des Wi-Fi-Stacks durch Google Project Zero

4.4 Erpressung im Zielfahrzeug

Wurde die Ransomware erfolgreich installiert und ausgeführt, kann die eigentliche Geiselnahme beginnen. In diesem Fall ist die Geisel sinnbildlich:

- Eine gesperrte kritische Fahrzeugkomponente, die nicht so leicht wiederhergestellt bzw. umgangen werden kann oder nicht lange ausfallen darf
- Die Beschlagnahmung oder das Durchsickern kritischer Fahrzeugdaten, die nicht einfach wiederhergestellt werden können oder die einen erheblichen Schaden verursachen würden, wenn sie öffentlich zugänglich wären
- Jede andere Behauptung, um das Opfer zur Zahlung des Lösegelds zu zwingen (z.B. reine Behauptung, es sei etwas gesperrt worden)

Sobald einmal der Zugriff gelungen ist, hat der Angreifer unzählige Möglichkeiten, um seine Epressungsaktion durchzuführen. In Abbildung 1 sind mögliche Systemkomponenten dargestellt, welche sich zum Bricken, Sperren oder Leaken anbieten würden.

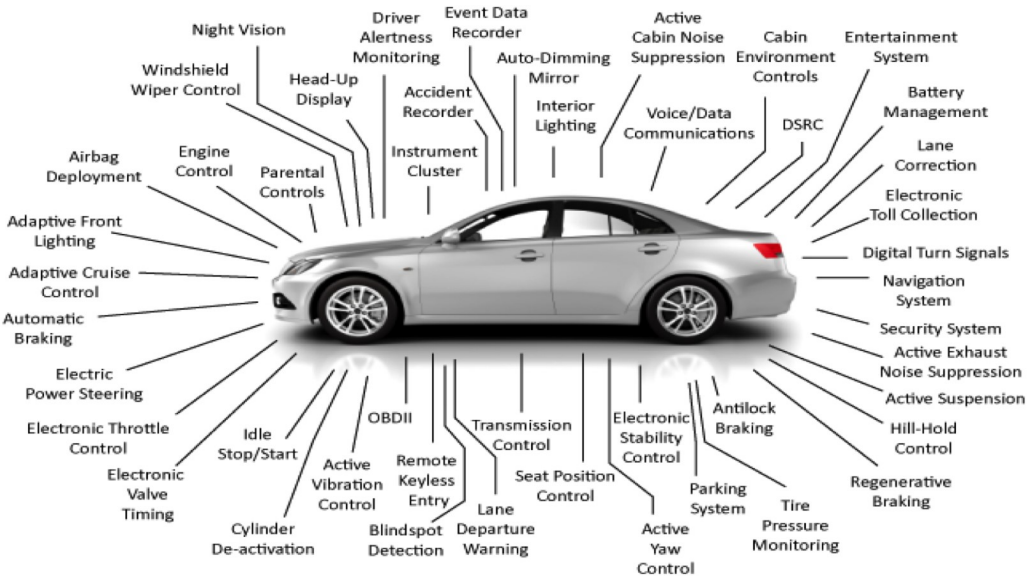

Abbildung 1: Mögliche Systemkomponenten, welche durch eine Ransomware missbraucht werden könnten [4]

Abbildung 1 macht deutlich, dass es in heutigen Autos zahlreiche Systeme gibt, auf denen man einen Cyber-Angriff durchführen kann. Sei es das Blockieren wichtiger Steuergerätfunktionen oder kryptografischer Anmeldeinformationen, das Verschlüsseln von kritischen Daten, das Freigeben kritischer interner Daten im Fahrzeug, das Manipulieren von Sensor-/Servodaten oder das Manipulieren bzw. Zerstören kritischer Fahrzeugkomponenten – ein Angreifer hat viele Möglichkeiten.
Sobald die Geiselnahme durchgeführt oder vorgetäuscht wurde, wird die Ransomware für das Opfer sichtbar. Eine solche Erpressungsmeldung erklärt in der Regel die eigentliche Erpressungssituation klar und deutlich und gibt sehr detaillierte Anweisungen und Informationen, wie das geforderte Lösegeld zu zahlen ist. Zur Demonstration haben die Autoren eine solche Meldung erstellt, welche in Abbildung 2 zu sehen ist.

Abbildung 2: Beispielhafte Erpressungsmeldung mit Zahlungsinformationen [2]

4.5 Ablauf der Lösegeldzahlung und Freigabe des Zielfahrzeugs

Wenn man die ganze Situation etwas genauer betrachtet, dann zeichnet sich ab, dass dieses Vorgehen eher für gewerbliche und öffentliche Fahrzeuge geeignet ist. In den meisten Fällen würde eine Privatperson keine absolute Dringlichkeit haben, das Auto sofort wieder in einen funktionierenden Zustand zu bringen, sondern eher Werkstattexperten zur Hilfe holen und keineswegs große Lösegeldsummen zahlen. Unternehmen mit großen Fahrzeugflotten sind hingegen vielversprechende Opfer, da diese auf ihre Fahrzeuge angewiesen sind und bei einem Ausfall mit großen Verlusten zu rechen ist. Dementsprechend stellen folgenden Fahrzeugtypen deutlich lukrativere „Lösegeldopfer“ dar:

- Lkw's mit ihren engen Zeitplänen, empfindlichen Gütern und hohen Vertragsstrafen
- Reisebusse mit ihren ähnlich engen Zeitplänen, die bis zu 70 Passagiere schnellstmöglichst transportieren müssen
- Landmaschinen, die Millionen $ kosten, aber nur einige Wochen im Jahr auf dem Feld eingesetzt werden
- Baufahrzeuge oder andere Spezialfahrzeuge mit komplexer, teurer und gefährlicher Ausrüstung
- Behördenfahrzeuge, die für die öffentliche Sicherheit wichtig sind, wie z.B. Polizei-, Feuerwehr- oder Krankenhausfahrzeuge
- Autovermietungen oder Autoleasingfirmen, aber auch große firmeneigene Fahrzeugflotten oder ein Fahrzeughersteller selbst
- Militärfahrzeuge

Angenommen, eines der oben genannten Fahrzeuge wäre infiziert und das Opfer ist bereit, das Lösegeld zu zahlen, ist es von essentieller Bedeutung, dass der Ransomware-Client einen schnellen, einfachen, benutzerfreundlichen und anonymen Zahlungskanal bereitstellt. Am besten eignet sich eine kryptische Währung wie z.B. Bitcoin oder Ethereum. Mittlerweile existieren Smartphone-Apps, welche praktisch alle physischen Währungen in anonyme Kryptowährungen umwandeln und transferieren.
Damit das Fahrzeug nach einer erfolgreichen Bezahlung wieder freigegeben werden kann, muss beim Bezahlvorgang eine eindeutige Fahrzeugkennung erstellt werden. Nur so ist es am Ende für den Erpresser möglich zu erkennen, welches Fahrzeug wieder entsperrt werden muss. Eine solche Identität kann in das Zahlungsschema eingebunden werden, indem jedes Fahrzeug eine individuelle Zahlungszieladresse besitzt oder der Ransomware-Client sendet eine verschlüsselte individuelle Nachricht an seinen Bot-Master.
Ist eine Zahlung beim Erpresser eingegangen, dann muss dieser nochmals eine Verbindung mit dem entsprechenden Ransomware-Client aufnehmen, um diesem den Entsperrbefehl zu senden und das Fahrzeug im besten Fall wieder freizugeben.

5 Präventivmaßnahmen gegen fahrzeugbezogene Ransomware

Wie bereits erläutert, gibt es unzählige Möglichkeiten, ein Fahrzeug mittels Ransomware zu attackieren. Dementsprechend gibt es auch keine allumfassende Schutzmaßnahme. Vielmehr benötigt man ein ganzheitliches Security-Engineering-Konzept, das einen vollständigen, systematischen und mehrschichtigen Schutzansatz verfolgt. Dieses Konzept umfasst:

- Das komplettes Fahrzeugsystem (d.h. vom einzelnen Steuergerät bis zum angeschlossenen Cloud-Backend)
- Den gesamten Fahrzeuglebenszyklus (d.h. von der ersten Anforderungsanalyse bis zur Ausmusterung des Fahrzeugs)

- Die komplette Fahrzeugorganisation (d.h. von den Sicherheitsprozessen bis zur Security Governance)

Dies wiederum gestaltet sich als schwierig und kostspielig im Gegensatz zu klassischen IT-Systemen, da Fahrzeuge deutlich mehr Angriffspunkte haben, keine effektive Sicherung von Daten oder Funktionen durchführen können, in den meisten Fällen keine regelmäßigen Sicherheitsupdates erhalten und nur eine einfache Firewall besitzen.

5.1 Absicherung des gesamten Fahrzeugsystems

Da man davon ausgehen muss, dass ein Angreifer das Zielfahrzeug nach der schwächsten Komponente absuchen würde, muss bei der Absicherung das gesamte Fahrzeug betrachtet werden. Das heißt, dass man von jedem einzelnen Steuergerät bis hin zu angeschlossenen Backend-Diensten alles betrachtet.
Des Weiteren ist es von Vorteil, gleichzeitig mehrere Verteidigungslinien zu haben, da man davon ausgehen muss, dass eine der Schutzmaßnahmen geschwächt wird oder ausfällt.
Einen Schutzansatz nach dem „Singel Point of Failure“ Prinzip, sollte man definitiv vermeiden. Dieser geht davon aus, dass eine einzige Komponente (z.B. Firewall) das gesamte sichere interne Fahrzeugnetzwerk von einem unsicheren, externen Netzwerk isoliert. Sollte ein Angreifer in dieser Komponente eine Schwachstelle entdecken, hätte das zur Folge, dass auf einmal alle Fahrzeuge des betroffenen Typs komplett kompromittiert würden.
Um ein solches Szenario zu verhindern und entgegenzuwirken muss der Angriffspfad so oft wie möglich durchbrochen werden. Dazu empfehlen die Autoren folgende Maßnahmen:

- Fahrzeug-Cybersicherheit Intelligenz & Forschung
- Klassische Unternehmenssicherheit für alle Fahrzeug-IT-Infrastrukturen
- Starke Backend-Zugriffskontrolle für alle fahrzeugbezogenen Assets, Schnittstellen und Funktionalitäten
- Vollständiger Schutz der Fahrzeugschnittstellen
- Sichere Fahrzeug-E/E-Architektur
- System zur Erkennung und Verhinderung von Eindringlingen in das Fahrzeug
- Fahrzeuginterne Firewall
- Verfahren zur Reaktion auf Vorfälle

5.2 Absicherung des gesamten Fahrzeuglebenszyklus

Neben der Absicherung des gesamten Fahrzeugsystems muss auch der gesamte Fahrzeuglebenszyklus betrachtet werden. Dieser erstreckt sich vom Start der Entwicklung bis zur Ausmusterung des Fahrzeugs. Dies garantiert, dass man auf die sich ständig ändernden Sicherheitsanforderungen schnellstmöglich reagieren kann und somit neu entdeckte Schwachstellen beheben und neu entwickelte Sicherheitsansätze einbringen kann.
Ein solcher kontinuierlicher Lebenszyklus hat auch einige zusätzliche technische und organisatorische Implikationen. Die gesamte Entwicklungshardware, alle Werkzeugketten und zumindest ein Teil der beteiligten Experten müssen bis zur endgültigen Ausmusterung verfügbar bleiben, was für schwere Nutzfahrzeuge einen Zeitraum von bis zu 20 Jahren bedeutet.

5.3 Absicherung der gesamten Fahrzeugorganisation

Die letzte Komponente im mehrschichtigen Schutzansatz behandelt die Absicherung der gesamten Fahrzeugorganisation und erfordert eine tiefe, bereichsübergreifende Integration und ein starkes Engagement der gesamten Organisation, einschließlich dediziertem Budget, Mitarbeitern und Befugnissen.
Eine gut aufgestellte Sicherheitsorganisation kann die Sicherheitsrisiken durch die Verringerung der Komplexität reduzieren, einen guten Systemüberblick bieten und für eine ordnungsgemäße Verwaltung aller sicherheitskritischen Funktionen und der entsprechenden Berechtigungsnachweise sorgen.

6 Maßnahmen gegen fahrzeugbezogene Ransomware

Ist der Fall eingetreten, dass man Opfer eines Ransomware-Angriffs geworden ist, empfehlen Experten, das Lösegeld auf keinen Fall zu bezahlen. Oft erfolgt, trotz Zahlung des geforderten Lösegeldes, keine Entsperrung des Fahrzeugs. Ebenso wird verhindert, dass dieses Vorgehen Nachahmer fördert.
Um aber nun das Fahrzeug bzw. die Fahrzeugflotte wieder in einen fahrtauglichen Zustand zu versetzen und somit größere finanzielle Schäden zu verhindern, empfehlen die Autoren einen neunstufigen Notfallplan. Unter der Voraussetzung, dass ein erfahrenes Fahrzeugsicherheitsexpertenteam, ein fahrzeugspezifischer Sicherheits-Notfallplan und eine Remote-Software-Update-Funktionalität vorhanden sind, wird folgendes Notfallverfahren empfohlen:

1. Möglichst frühzeitige Erkennung von Fahrzeug-Ransomware durch Meldungen erster Opfer oder durch das Cyber-Security-Intelligence Team des Unternehmens
2. Analysen von Fahrzeug-Ransomware durch Fahrzeugsicherheitsexperten
3. Sicherheitsrisiko- und Schwachstellenbewertung durch Fahrzeugsicherheitsexperten auf Basis einer systematischen Auswertung für entsprechende Angriffspotenziale
4. Identifizierung und Bewertung möglicher Gegenmaßnahmen und Reaktionen, einschließlich der Zahlung des geforderten Lösegelds
5. Entscheidung der Unternehmensleitung auf Basis der Vorschläge der Sicherheitsexperten für Reaktionsmaßnahmen (z. B. technische und nicht-technische Maßnahmen), Incident Response Communication, weitere Risikovorsorge, etc.
6. Entwicklung, Test und Vorbereitung von:
    a) Technischen Reaktionsmaßnahmen wie z.B. die Bereitstellung von Steuergeräte-Backup-Firmware, Fahrzeug- und/oder Infrastruktur-Software-(Sicherheits-)Patches, Steuergeräte-/Fahrzeug- Neukonfigurationsbefehle
    b) Nicht-technischen Reaktionsmaßnahmen wie Angreifer-Diplomatie, Lösegeldzahlung, Informieren allgemeiner Cyber-Abwehrbehörden
    c) Incident Response-Kommunikation innerhalb des Unternehmens und gegenüber Kunden, Lieferanten, Partnern, Branchengremien, Behörden oder Medien
7. Roll-out von technischen und nicht-technischen Reaktionsmaßnahmen und Beginn der Incident-Response- Kommunikation
8. Kontinuierliche Überwachung und (Neu-)Bewertung von Auswirkungen, Risiken und Erfolg aller durchgeführten Reaktionsmaßnahmen zur Anpassung von Maßnahmen oder weiteren/wenigeren Maßnahmen
9. Untersuchung und Sicherheitsforensik zur Dokumentation und Berichterstattung, vor allem aber zur langfristigen Eindämmung, vollständigen Wiederherstellung, Lessons-Learned, Präventionsmaßnahmen und aktualisierten Überwachung.

7 Schluss/Fazit

Aktuell sind Ransomware-Angriffe auf Fahrzeuge noch Theorie, doch schon in naher Zukunft kann sich dies ändern. Aufgrund der zunehmenden Digitalisierung und Konnektivität von Autos bieten sich den Angreifern viele Angriffsflächen, welche, wenn die Automobilindustrie ihren Securityansatz nicht um den Aspekt Ransomware erweitert, schon bald rigoros ausgenutzt werden könnten. Hinter Ransomware-Angriffen steckt ein überzeugendes Geschäftsmodell und wenn man dadurch viel Geld verdienen kann, wird es auf kurze oder lange Sicht Personen geben, die sich dies zum Vorteil machen möchten.
Ziele werden weniger Privatpersonen werden, sondern eher Nutzfahrzeuge und große Fahrzeugflotten, da diese meist auf ihre Fahrzeuge angewiesen sind und sich keine lange Ausfalldauer leisten können.
Es ist unabdingbar, dass sich die Automobilindustrie auf Ransomware-Angriffe vorbereiten muss, indem sie die Schutzfunktionen in gleichem Tempo auf Fahrzeuge ausweitet, sich mit ganzheitlichen, mehrschichtigen Schutzmaßnahmen auf die Bedrohung vorbereitet, aber auch die Fähigkeit, mit aktualisierten Abwehrmaßnahmen und Reaktionen auf Angriffe zu reagieren, auf Fahrzeuge ausweitet.
Dieses Paper gibt nur einen kleinen Einblick in das Thema fahrzeugbezogene Ransomware-Angriffe. Aufgrund der begrenzten Seitenanzahl konnten nicht alle Aspekte erwähnt oder tiefgründiger diskutiert werden aber das Themengebiet bietet enorm viel Potential, in welchem tiefgründigere Forschungen getätigt werden können, um somit der Sicherheit für Autos beizutragen.

Literaturverzeichnis

[1] E. C., “Ransomware fakten, trends & statistiken 2021,” *Safety Detectives*, 24.05.2020. [Online]. Available: https://de.safetydetectives.com/blog/ransomware-fakten-trends-statistiken/

[2] M. Wolf, R. Lambert, A. Schmidt, and Thomas Enderle, “W anna d rive ? feasible attack paths and effective protection against ransomware in modern vehicles,” 2017.

[3] A. Greenberg, “Hackers reveal nasty new car attacks–with me behind the wheel (video),” *Forbes*, 24.07.2013. [Online]. Available: https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

[4] SnapEDA Blog, “What design engineers should know about procurement in automotive electronics - snapeda blog,” 2014. [Online]. Available: https://blog.snapeda.com/2014/03/03/procurement-in-automotive-electronics/