Vortäuschen von Komponentenfunktionalität im Automobil: Safety- und Komfort-Implikationen durch Security-Verletzungen am Beispiel des Airbags

Tobias Hoppe, Jana Dittmann
Arbeitsgruppe Multimedia and Security, Institut ITI der Fakultät für Informatik
Otto-von-Guericke Universität Magdeburg
Universitätsplatz 2
39106 Magdeburg
{tobias.hoppe, jana.dittmann}@iti.cs.uni-magdeburg.de

Abstract: Mit der Betrachtung gezielter Angriffe auf IT-Komponenten im Automobil rückt zunehmend auch der IT-Security-Aspekt im Automobil in den Fokus der Forschung. In diesem Beitrag wird in einem praktischen Black-Box Angriffsszenario an aktueller automotiver Hardware untersucht, ob und wie leicht ein Angreifer einen Angriff realisieren könnte, ohne dass ihm dazu interne Dokumente zur Verfügung gestellt werden. Bei der konkret betrachteten Angriffstechnik wird gegenüber dem Gesamtsystem und dem Anwender das Vorhandensein und der fehlerfreie Betrieb einer entfernten bzw. deaktivierten Komponente vorgetäuscht. Anhand des Beispiels eines entfernten Airbagsystems werden Schwachstellen identifiziert, die derartige Angriffe ermöglichen, mögliche Auswirkungen auf Safety und Komfort herausgestellt und der Bedarf für zukünftige, sichere automotive Bussysteme und Kommunikationsnetze motiviert.

Keywords: Entwicklung und Betrieb sicherer Systeme, Eingebettete Systeme, Angriffe, Automotive IT, Steuerung sicherheitsrelevanter Prozesse, Safety, IT-Security, Komfort

1 Einleitung und Motivation

Aktuelle Automobile werden zunehmend komplexer und bieten mehr und mehr Funktionen zugunsten des Komforts als auch der Sicherheit. Klassischerweise wird im automotiven Bereich die Sicherheit hauptsächlich im Sinne der Safety (Schutz im Kontext von Unfällen und Komponentenversagen) betrachtet. Zunehmend rückt jedoch auch der Aspekt der Security (Schutz vor beabsichtigten Angriffen) in den Fokus der aktuellen Forschung (z.B. [Kas05], [WWW], [GP06]), zumal sich die durch beabsichtigte Angriffe auf automotive IT erzielbaren Security-Verletzungen gerade im Automobil ebenso auf Komfort und Safety auswirken können.

In [LDKH] und [HD07] haben wir bereits gezeigt, dass Angreifer auch in aktuellen automotiven IT-Strukturen die fünf grundlegenden Angriffs-Strategien (Unterbrechen, Lesen, Spoofing, Modifizieren, Löschen) schon in einfachen Kombinationen wirksam einsetzen können. In diesem Beitrag betrachten wir ein komplexeres Schema automotiver IT-Angriffe, das Vortäuschen von Komponentenfunktionalität, und untersuchen entsprechende IT-Security-Angriffe auf ihre Safety- und Komfort-Wirkung.

Für unsere Untersuchungen definieren wir den Begriff des Vortäuschens wie folgt und grenzen ihn dabei gegen die ähnliche Strategie der Simulation ab. Wir beziehen uns dabei auf den Kontext automotiver IT-Angriffe, bei dem es dem Angreifer gelingt, eigene Steuerlogik in Form von Hard- oder Software in das automotive Gesamtsystem einzubringen und dadurch ggf. bestehende Hard- oder Software zu ersetzen.

Simulation von Komponentenfunktionalität: Die ersetzte Hard- oder Software-Komponente des Angreifers behält die eigentliche Funktionalität der betroffenen Komponente vollständig bei, so dass der Angriff in Bezug auf diese Komponente keine merklichen Auswirkungen (z.B. auf Komfort oder Safety) hat. Zusätzlich ist jedoch weitere, ungewünschte Funktionalität enthalten, die anderweitig den Zwecken des Angreifers dient und so die IT-Security des Gesamtsystems beeinträchtigt, was ebenfalls Auswirkungen auf Safety und Komfort haben kann. Beispielsweise könnte eine originale Hardwarekomponente komplett durch eine mit erweitertem Funktionsumfang ersetzt oder bei einem bestehenden Gerät lediglich die Betriebssoftware gegen eine mit zusätzlichen Schadfunktionen getauscht werden.

Vortäuschen von Komponentenfunktionalität: Die Kern-Funktionalität der ersetzten Komponente ist nach dem Angriff nicht mehr vorhanden. Dies kann über zwei letztendlich äquivalente Ansätze realisiert sein: a) die Komponente wird entfernt und ist im Automobil folglich physisch nicht mehr existent oder b) die Komponente ist noch im Automobil angeschlossen, wird jedoch anderweitig inaktiv gesetzt. Dadurch hat ein solcher Angriff unmittelbare Auswirkungen auf von dieser Komponente realisierte Komfort- und Safety-Eigenschaften. Um das effektive Wegfallen der Komponente den weiteren Geräten im Verbund und damit letztendlich auch dem Anwender so weit wie möglich vorzuenthalten, wird dagegen durch einen weiteren Eingriff an dieser oder einer anderen Stelle des Automobils (z.B. durch Hinzufügen schadhafter Hard- oder Software) lediglich nach außen ein normaler Betriebszustand der Komponente vorgetäuscht.

Wir konzentrieren uns in diesem Beitrag auf den Aspekt des Vortäuschens. Diesen konnten wir in einem praktischen Black-Box Angriffsszenario (d.h. äquivalent zu einem Großteil der Angreifer ohne die Bereitstellung von Spezifikationen durch den KFZ-Hersteller) im Labor an aktueller automotiver IT nachvollziehen und auf seine Folgen für Safety und Komfort untersuchen.

In Kapitel 2 werden als Stand der Technik einige ausgewählte automotive Komponenten vorgestellt und auf ihre Safety- und Komfort-relevanten Eigenschaften hin untersucht. Nach der Vorstellung der Versuchsumgebung in Kapitel 3 folgt die Beschreibung der im Zuge des praktischen Black-Box Angriffsszenarios vorgenommenen Schritte in Kapitel 4. Kapitel 5 liefert eine Analyse der zugrunde liegenden Ursachen und einen Ausblick auf zukünftige Gegenmaßnahmen, bevor der Beitrag in Kapitel 6 mit einer Zusammenfassung der gewonnenen Erkenntnisse endet.

2 Stand der Technik

Als Beispiele für typische automotive Komponenten werden in Tabelle 1 einige exemplarisch ausgewählte Systeme aufgezählt. Dabei werden einige wesentliche Aspekte ihrer Bedeutung für Safety und Komfort aufgeführt.

Komponente	***Safety-Funktionen***	***Komfort-Funktionen***
Klimaanlage	*(kein direkter Einfluss auf Safety, jedoch ggf. indirekt durch Unfälle bedingt durch Ablenkung des Fahrers aufgrund schwerer, unintuitiver Bedienung oder schlechtem Befinden aufgrund ungeeigneter Klimatisierung)*	Angenehme Temperierung nach den Wünschen der Insassen
ABS / ESP-System	Fahrwerkskontrolle (Bremsverhalten / Fahrzeugstabilität)	Erleichtern dem Fahrer geeignete Reaktionen in Ausnahmesituationen
Airbag-System	Passive Aufprallsicherheit	*(kein Einfluss auf Komfort)*
Zentralverriegelung	Kindersicherung Überfall-/Diebstahlschutz (Security)	Komfortables Öffnen oder Schließen aller Türen von einem Bedienelement

Tabelle 1: Exemplarische automotive Komponenten und ihre Safety- und Komfort-Funktionen

Von diesen beispielhaften automotiven Komponenten wurde für das im praktischen Versuchsaufbau durchgeführte Black-Box Angriffsszenario der Airbag als betrachtetes System exemplarisch ausgewählt, um die Angriffsvariante des Vortäuschens beispielhaft zu veranschaulichen und auf ihre Auswirkungen auf Safety und Komfort zu untersuchen. Nach der Vorstellung der Testumgebung im folgenden Kapitel 3 folgt die detaillierte Beschreibung im anschließenden Kapitel 4.

3 Versuchsaufbau

Die Versuchsumgebung besteht aus einem Kabelbaum und verschiedenen Steuergeräten eines aktuellen Modells (Baujahr 2004) eines großen internationalen Automobilherstellers. Fahrzeuge dieser Modellreihe nutzen die CAN Bus Technologie [CAN] zur Vernetzung der einzelnen automotiven Komponenten. Eine schematische Darstellung des Versuchsaufbaus ist in Abbildung 1 dargestellt.

Neben den rein automotiven Komponenten, wie den hier beispielhaft dargestellten Steuergeräten *A*, *B* und *C*, einen die verschiedenen CAN Bus Subnetzwerke verbindenden Gateway *G* und der Instrumentenkombination *I,* gehört des Weiteren ein Laptopsystem *L* zu dem Versuchsaufbau. Dieses kann über Hardware-Interfaces sowohl zur On-Board Diagnoseschnittstelle (OBD II) *D* als auch zu verschiedenen automotiven Bus-Systemen an das Bordnetzwerk des Testfahrzeuges angeschlossen werden.
Eine Diagnose des automotiven Systems bzw. seiner Komponenten kann so über ein verbreitetes Fahrzeugdiagnose-Produkt (Tester *T*) durchgeführt werden, das für Modelle des vorliegenden Fahrzeugherstellers ausgelegt ist.
Gleichzeitig kann dieses PC-System über eine entsprechende CAN-Interface-Box an beliebigen Stellen der Netzwerktopologie sowohl lesend als auch schreibend in die Kommunikation eingreifen. Dadurch kann z.B. ein infiziertes Steuergerät simuliert werden, welches bösartig in die Kommunikation des Gesamtsystems eingreift. Zur

Analyse und Interaktion auf Busebene mit der automotiven Testhardware wird dazu das Produkt CANoe von Vector-Informatik [Vec07] eingesetzt, das auch vielfach in der Automobilindustrie zu Entwicklungs-, Simulations- und Analysezwecken eingesetzt wird. Alternativ stehen auch Entwicklerplatinen zur Verfügung, mit denen ein entsprechend manipuliertes Steuergerät anstatt der Simulation über ein PC-System auch mit für automotive IT typischen Ressourcen nachgebildet werden kann.

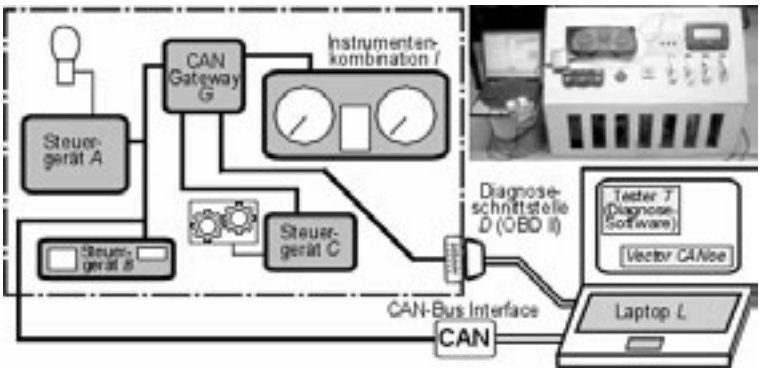

Abbildung 1: Skizzierung des Versuchsaufbaus: automotive Hardware und Test-Laptop

4 Ein praktisches Black-Box Angriffsszenario

Im betrachteten Szenario entfernt ein Angreifer physisch eine Komponente des automotiven Systems[1]. Als exemplarische Zielkomponente wurde das Airbagsystem gewählt. Der Angreifer könnte in diesem Fall beispielsweise ein krimineller Mitarbeiter einer Service-Werkstatt sein, der aus finanzieller Motivation handelt, indem er durch den Weiterverkauf der Hardware Gewinne erzielt. Eine andere Möglichkeit wäre ein Saboteur als Angreifer, der einen Unfall provoziert und die Personenschäden zu maximieren sucht. Eine detaillierte Analyse der Angreifertypen, ihrer Motivationen und Ziele wurde anhand der CERT-Taxonomie (nach [HL98]) von uns in [HD07] speziell für den Kontext automotiver Systeme angepasst und vorgestellt sowie in [HKLD] zusätzlich formalisiert. In diesem Beitrag wird gegen Ende von Abschnitt 4.2 noch einmal auf diese Klassifikation Bezug genommen. Bei beiden soeben betrachteten Angreifertypen liegt es in ihrem Interesse, dass das Entfernen des Airbags für Fahrzeughalter, -führer, sonstige Nutzer oder Servicepersonal zunächst möglichst wenig offensichtlich ist. Der faktische Wegfall von Komponenten wie Steuergeräten oder häufig bereits auch einzelner Leuchten (z.B. solcher, die dem Fahrer eine entsprechende Ausfall-Warnung signalisieren sollen), führt in der Regel zusätzlich auch zur Speicherung digitaler Fehlercodes im Automobil. Daher werden im Zuge unserer Untersuchungen

[1] Wie es als Fall b) in der Definition des Vortäuschens in Kapitel 1 aufgeführt ist, könnte der Angreifer die gewählte(n) Komponente(n) dazu statt des physischen Entfernens auch anderweitig deaktivieren. Obgleich die in diesem Abschnitt beschriebenen Techniken dort anschließend ähnlich eingesetzt werden könnten, wird dieser Fall hier jedoch nicht weiter betrachtet

insbesondere IT-basierte Angriffe untersucht, über die ein Angreifer die entfernten Komponenten elektronisch nachbildet, um ihr Verhalten auch gegenüber dem Rest des Systems vortäuschen und so ihren Verlust zu verbergen.

Dazu werden im folgenden Abschnitt 4.1 die wesentlichen Symptome betrachtet, anhand derer sich das Fehlen des Airbagsystems im exemplarisch betrachteten Fahrzeugtyp äußert. Anschließend werden in Abschnitt 4.2 praktische Techniken identifiziert, mit denen der Angreifer eine Unterdrückung dieser Symptome auf dem vorliegenden System erreichen könnte. Im Zuge eines praktischen Black-Box Angriffsszenarios werden abschließend in Abschnitt 4.3 die relevanten Auswirkungen des betrachteten IT-Security-Angriffs auf Safety und Komfort analysiert.

4.1 Identifikation der wesentlichen Symptome nach dem Entfernen

Mit Bezug auf den vorliegenden Versuchsaufbau konnten folgende wesentliche Symptome identifiziert werden, anhand derer ein Fehlen der Airbagkomponenten noch rechtzeitig vor einem Ernstfall[2] bemerkt werden könnte:

- Die Airbag-Warnleuchte in der Instrumentenkombination ist aktiv
- Das Airbag-Steuergerät antwortet nicht während einer Fahrzeugdiagnose
- Die Lücke im Verbauort wird entdeckt

Die Reihenfolge der Aufzählung orientiert sich an der Wahrscheinlichkeit, zu der der Angreifer mit einer Entdeckung rechnen müsste. Während die Warnleuchte als sehr eindeutiges Zeichen für den Angriff zu werten ist, ließe sich das Risiko einer zufälligen Entdeckung des physischen Fehlens der Komponenten am ehesten vernachlässigen.

4.2 Vortäuschen der Komponentenfunktionalität

In diesem Abschnitt werden am Versuchsaufbau praktisch nachvollzogene Maßnahmen untersucht, mit denen der Angreifer das Fehlen der entfernten Komponenten zu tarnen versuchen könnte. Die drei im vorigen Abschnitt 4.1 identifizierten Symptome werden dabei einzeln adressiert. Unter dem Titel *Angriffsteil 1* wird in diesem Abschnitt zunächst das Vortäuschen der entfernten Komponente während der Fahrzeugdiagnose und damit der zweite Fall vertieft behandelt. Anschließend werden mit *Angriffsteil 2* und *Angriffsteil 3* ausgewählte potenzielle Techniken des Angreifers zur Berücksichtigung der beiden weiteren Angriffsziele kurz vorgestellt.

Angriffsteil 1: Bereitstellen eines regulären Zustands bei einer Fahrzeugdiagnose

Das in diesem Abschnitt betrachtete Ziel des Angreifers ist es, dass sich das entfernte Airbag-Steuergerät trotz des Ausbaus bei einer Fahrzeugdiagnose identifizieren und als fehlerfrei erkennen lässt. Wie es auch zum Erreichen einiger seiner weiteren Ziele (s.u.)

---

[2] Der bereits als potenzieller Angreifer identifizierte Saboteur könnte zusätzlich noch versuchen, ggf. *post-incident* stattfindende Ermittlungen zu erschweren (z.B. durch rein software-basierte Realisierungen, bei denen der Schadcode ausschließlich aus dem flüchtigen Arbeitsspeicher agiert und dadurch nach einer Unterbrechung der Stromversorgung nicht mehr nachweisbar ist). Dieser Fall kann hier jedoch nicht weiter vertieft werden.

erforderlich ist, muss der Angreifer dazu direkt in die Systeme des Fahrzeugs und ihre Kommunikation eingreifen. Abbildung 2 zeigt sowohl den Normalfall einer Diagnose des Airbagsteuergerätes *A* (z.B. Airbag-Steuergerät) durch den Tester *T* als auch angesichts zweier potenzieller Szenarien, über die der Angreifer einen derartigen Angriff konzipieren könnte. Den dazu notwendigen Programmcode bringt der Angreifer selbst in das Fahrzeug ein, wozu ihm beispielsweise das Anklemmen einer kleinen programmierbaren Platine mit CAN-Controller (*A'*) an die Busleitungen des jeweiligen Subnetzes genügt (z.B. anstelle des entfernten Gerätes *A*). Alternativ könnte er ohne Notwendigkeit zusätzlicher Hardware auch den Code einer bestehenden Komponente *B* mit Zugriff auf dieses Subnetz entsprechend modifizieren, sofern ihm (beispielsweise über unzureichend abgesicherte Flash-Schnittstellen) entsprechende Zugriffe möglich sind. Dabei würde analog zum in Kapitel 1 vorgestellten Ansatz der Simulation die vorgesehene Funktionalität der Komponente *B* beibehalten werden. Durch die zusätzlichen Schadfunktionen würde nun jedoch das abgeänderte Steuergerät *B'* auch die Diagnoseanfragen für das entfernte Gerät *A* beantworten und so dessen Vortäuschung unterstützen. Im vorliegenden Versuchsaufbau (vgl. Kapitel 3) wurde der erstere dieser Ansätze verfolgt, wobei die angefügte Schaltung in diesem Versuchsaufbau durch den über die CAN-Schnittstelle angeschlossenen Laptop nachgebildet wurde.

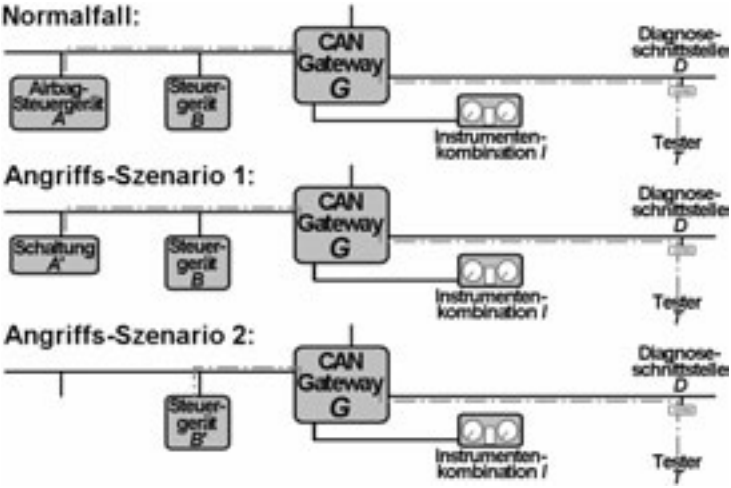

Abbildung 2: Ablauf einer Diagnosesitzung im Normalfall und angesichts zweier exemplarischer Angriffs-Szenarien

Um dem in Abschnitt 3 vorgestelltem Diagnosewerkzeug die fehlerfreie Funktionalität des Airbagsystems vorzutäuschen, wird im Powertrain-Subnetz des automotiven Testsystems eine bösartige Komponente *A'* platziert, die Diagnoseanfragen an das Airbagsteuergerät *A* selbst entgegennimmt und zur Zufriedenheit des Testers beantwortet.

Entsprechend der Black-Box Anforderungen wurden uns seitens des gewählten Fahrzeugherstellers keine internen Spezifikationen oder anderweitig hinreichende Informationen zum eingesetzten Diagnoseprotokoll (sowie auch zur allgemeinen Buskommunikation) bereitgestellt. Daher wurde vorbereitend der typische Ablauf einer

solchen Diagnose-Sitzung über das CAN-Bus Interface ausgelesen, aufgezeichnet und analysiert. Weil die Übertragung offensichtlich unverschlüsselt erfolgt, lässt sich die Syntax und Semantik des Protokolls aus den aufgezeichneten Binärdaten mit vergleichsweise geringem Aufwand grob rekonstruieren. Das in Tabelle 2 beschriebene Kommunikations-Schema gibt einen pauschalisierten Überblick über den Ablauf der Diagnose-Sitzung durch einen Tester *T* einmal mit und einmal ohne Präsenz des zu diagnostizierenden Steuergerätes *A*.

Ablauf einer typischen Diagnosesitzung bei nicht vorhandenem Steuergerät		***Ablauf einer typischen Diagnosesitzung bei vorhandenem Steuergerät***	
Diagnose-Tester T	***Steuergerät A***	***Diagnose-Tester T***	***Steuergerät A***
Anfrage zum Öffnen der Diagnosesitzung unter Adressierung von *A*	[keine Antwort]	Anfrage zum Öffnen der Diagnosesitzung unter Adressierung von *A*	Bestätigung + für die Sitzung verwendete Adressen
Anfrage zum Öffnen der Diagnosesitzung unter Adressierung von *A*	[keine Antwort]	Anfordern von Geräteinformationen (z.B. Teilenummer, Revision)	Angeforderte Daten
Anfrage zum Öffnen der Diagnosesitzung unter Adressierung von *A*	[keine Antwort]	Geräteinformationen von *A* dem Nutzer des Diagnosesystems anzeigen	
Anfrage zum Öffnen der Diagnosesitzung unter Adressierung von *A*	[keine Antwort]	Auf Anforderung des Nutzers Liste gespeicherter Fehlercodes von *A* abrufen	Liste gespeicherter Fehlercodezahlen (im Normalfall leer)
Ausgabe einer Fehlermeldung + Hinweis, dass das gewünschte Gerät *A* nicht antwortet.		Ergebnisliste anzeigen oder Hinweis, dass keine Fehlercodes auf *A* vorhanden sind.	

Tabelle 2: Ablauf einer typischen Diagnosesitzung ohne und mit vorhandenem Steuergerät

Im vorliegenden Fall reichen die gewonnenen Informationen aus, um eine rudimentäre Nachbildung der Diagnosefunktionalität eines Steuergerätes *A* des vorliegenden Automobilherstellers in der in CANoe verwendeten, C-ähnlichen Sprache CAPL zu implementieren. Die von diesem vorgetäuschten Gerät *A'* an den Tester *T* gesendeten Geräteinformationen (Gerätename, Teilenummer, Revision etc.) sowie die gemeldeten Einträge im Fehlerspeicher können dabei beliebig editiert werden. Nach dem Eintragen einer typischen Identität eines Airbagsteuergerätes *A* und eines entsprechenden leeren Fehlerspeichers kann diese schadhafte Komponente als *A'* analog zu Szenario 1 aus Abbildung 2 im entsprechenden CAN-Subnetz platziert werden. Fortan liefert sie im vorliegenden Versuchsaufbau gegenüber dem Tester *T* die erwarteten Geräteinformationen und täuscht bei einer Fehlercodeabfrage einen fehlerfreien Zustand des physisch nicht im Test-Setup vorhandenen Gerätes *A* vor.

Angriffsteil 2: Unterdrücken der Airbag-Warnleuchte

Wie schon einleitend in Abschnitt 4.1 erwähnt, gehört auch das Deaktivieren der Airbag-Warnleuchte in der Instrumentenkombination zu den Zielen des betrachteten Angreifers. Diese stellt das offensichtlichste Zeichen dar, über das der Fahrer auf eine Störung (in diesem Fall das Fehlen) des Airbag-Steuergerätes aufmerksam werden kann. Die Information über das Vorhandensein einer Störung des Airbagsystems bezieht die Instrumentenkombination *I* (vgl. Abbildung 2) im vorliegenden Fahrzeug über den zentralen CAN-Gateway *G*, der zweimal pro Sekunde eine entsprechende Information in

das Subnetz der Instrumentenkombination absendet.
Der direkte Ansatz gemäß der vorgestellten Strategie des Vortäuschens wäre, die Anwesenheit und Fehlerfreiheit des Airbag-Steuergerätes *A* aus seinem eigenen Subnetz heraus vorzutäuschen. Die Autoren vermuten, dass ein Angreifer dies problemlos analog zur bereits im vorigen Abschnitt praktisch demonstrierten Technik realisieren kann, sobald er die dazu vom Airbag-Steuergerät auszusendenden Nachrichten und deren Syntax identifiziert hat. Dies gestaltete sich im vorliegenden, nicht in kompletter Ausführung vorhandenen Fahrzeugnetzwerk des Versuchsaufbaus zunächst noch schwierig. Daher wurden exemplarisch zwei weitere potenzielle Ansätze identifiziert und praktisch demonstriert, über die ein Angreifer dasselbe Ziel erreichen kann.
Als erste praktisch demonstrierte Angriffsstrategie zum Deaktivieren der Airbagleuchte wurde im vorliegenden Versuchsaufbau folgende Designschwachstelle identifiziert, über die ein Angreifer das Ziel komfortabel realisieren kann: Im Flash-Speicher des zentralen CAN-Gateways *G* befindet sich ein Kodierungsfeld, das u.a. eine Verbauliste beinhaltet. Dieses lässt sich ohne Notwendigkeit eines Passwortes über die verwendete Diagnose-Software editieren und dadurch das Airbag-System aus der Verbauliste entfernen. Anschließend wertet der CAN-Gateway *G* das Fehlen des Airbagsystems *A* nicht mehr als Fehler und stellt das Senden der Fehlerkennung ein. Die Leuchte zur Anzeige von Airbagstörungen in der Instrumentenkombination *I* erlischt sofort und das Fehlen des Airbagsystems *A* ist für den gewöhnlichen Nutzer fortan nicht mehr ersichtlich.
Ein weiterer entsprechender Angriff, der ebenfalls am Versuchsaufbau nachvollzogen werden konnte, besteht im Einspielen gefälschter CAN-Telegramme in das CAN-Subnetz, in dem sich die Instrumentenkombination *I* befindet. Dies erfolgt, indem unmittelbar auf die zweimal pro Sekunde vom Gateway *G* gesendete Statusinformation (s.o.) eine inhaltlich entgegengesetzte eingefügt wird. Aus technisch noch nicht abschließend geklärten Gründen konnte in diesem Versuch, wenn auch nur phasenweise, ein kurzzeitiges Aufflackern der entsprechenden Leuchte wahrgenommen werden. Dennoch resultiert dieser Angriff phasenweise auch in einem kompletten Erlischen der Warnleuchte in der Instrumentenkombination *I*, so dass letztendlich auch die Wirksamkeit dieses alternativen Ansatzes prinzipiell gezeigt werden konnte.

Angriffsteil 3: Tarnung der Lücke im Verbauort

Das letzte identifizierte Anzeichen, das im Nachhinein Aufmerksamkeit erregen und damit letztlich zur Entdeckung des Angriffs führen könnte, ist die Lücke im Verbauort des Gerätes *A*, sofern dieses durch den Angreifer komplett entfernt und nicht lediglich inaktiv gesetzt wurde (vgl. Fall a) und b) aus der Definition des Vortäuschens in Kapitel 1). Diese kann der Angreifer vergleichsweise sehr einfach gegen zufällige Entdeckung tarnen, indem er eine Attrappe wie z.B. ein entsprechendes defektes Gerät einsetzt.

Wie es sich auch praktisch am vorliegenden Versuchsaufbau nachvollziehen ließ, ist es durch die in diesem Kapitel vorgestellten Schritte möglich, das Entfernen und die faktische Nicht-Funktionalität des Airbagsystems sowohl vor dem normalen Nutzer als auch geschultem Werkstattpersonal zu verbergen, zumindest solange kein gezielter Verdacht eines entsprechenden Vorfalls aufgekommen ist. Da gerade das Airbagsystem sich jedoch bis zu einem Ernstfall für den Nutzer sehr unscheinbar verhält, ist das Risiko einer (rechtzeitigen) Erkennung für den Angreifer in diesem Fall überschaubar. Abbildung 3 liefert eine grobe Einordnung des vorgestellten Angriffs-Szenarios in

seinen drei vorgestellten Schritten in das gegen Anfang von Kapitel 4 bereits kurz erwähnte CERT Klassifikationsschema ein. Hierbei ist hervorzuheben, dass bei den für diese Angriffsstrategie relevanten Angreifern im Allgemeinen kein Insiderwissen vorauszusetzen ist. Dies stellt jedoch gegenwärtig keine große Hürde dar, wie von uns im praktisch untersuchten Black-Box Angriffsszenario gezeigt werden konnte.

	Angreifer	Werkzeug	Schwachstelle	Aktionen	Ziel	Unautorisiertes Ergebnis	Motivation
Angriffsteil 1:	Dieb (ggf. Saboteur)	Schadcode, angehängtes Gerät	Design	Lesen, Einspielen	Steuergerät A, Tester T	Diebstahl von Ressourcen, Kompromittierung von Informationen / Programmen, Verletzung von Authentizität, Integrität, Verfügbarkeit etc.	Finanzielle Interessen (ggf. Freude am Schaden)
Angriffsteil 2:		Diagnosetool oder angehängtes Gerät	Design	Umkonfigurieren oder Lesen, Einspielen	Steuergeräte G+/		
Angriffsteil 3:		Attrappe		Einbau	Steuergerät A		

Abbildung 3: Klassifikation der Schritte des vorgestellten Angriffsszenarios nach CERT

4.3 Bewertung der Auswirkungen auf Komfort und Safety

Der in diesem Kapitel beschriebene Angriff kann auch über die unmittelbaren IT-Security-Verletzungen hinaus Auswirkungen auf das Fahrzeug und seine Umgebung haben. Dieser Abschnitt befasst sich mit der Identifikation derartiger indirekter Risiken, die über den finanziellen Schaden, die durch den Verlust der entwendeten Komponenten entstehen, hinausgehen. Dabei werden sowohl resultierende Einschränkungen des Komforts als auch der Safety betrachtet.

Potenzielle Auswirkungen auf den Komfort:

Prinzipiell können derartige Angriffe auch den Komfort des Fahrzeugs stark einschränken, sofern die entwendeten oder deaktivierten Komponenten auch dem Komfort dienen. Ein Diebstahl einer sehr komfortbezogenen Komponente wie z.B. der Klimasteuerung (vgl. Tabelle 1) könnte zwar äquivalent zum im vorigen Abschnitt behandelten Beispiel durch entsprechende Unterdrückung von Warnmeldungen und Bereitstellen gefälschter Diagnosefunktionalität technisch getarnt werden. Weil die Funktion der Klimaanlage jedoch für die Insassen unmittelbar spürbar ist, da sie schwerpunktmäßig dem Komfort dient (vgl. Abschnitt 2), hätte ein Angreifer bei einem entsprechenden Angriff schnell mit einer Erkennung des Vorfalls zu rechnen, bei der die Nutzer symptombezogen die Auswirkungen der Tat bemerken.

Potenzielle Auswirkungen auf die Safety

Noch schwerer wiegende Auswirkungen durch die beschriebene Angriffsstrategie können dagegen resultieren, wenn durch den Angreifer beiläufig oder ganz gezielt auch der Verlust von Safety-Funktionen in Kauf genommen wird. Wie auch das behandelte Beispiel des Airbag-Systems veranschaulicht, greifen diese Funktionen oft nur in Ausnahmesituationen ein, die lange Zeit nicht auftreten. Weitere Beispiele hierfür wären z.B. das ESP- oder ABS-System. In derartigen Fällen ist eine baldige symptombezogene Erkennung des Missstands durch den Nutzer seitens des Angreifers oft kaum zu befürchten, da die Wirksamkeit dieser Systeme nur selten spürbar wahrgenommen wird. Zudem kommt im Ernstfall die entsprechende symptomatische Erkennung des Versagens bzw. Fehlens von Safety-Funktionen bereits zu spät. Schwerwiegende Folgen

des Unfalls, die bei korrekter Funktion der kritischen Komponenten hätten verhindert werden können, sind in dieser Situation dann möglicherweise nicht mehr vermeidbar.

Wie sich in der praktischen Demonstration in Abschnitt 4.2 und der Analyse der möglichen Konsequenzen in diesem Abschnitt gezeigt hat, stehen gezielten Angriffen auf die IT-Sicherheit in aktuellen automotiven Systemen selbst ohne Voraussetzung von Insiderwissen bisher kaum wirksame Maßnahmen entgegen. Durch Angriffsstrategien wie dem in diesem Beitrag verfolgten Ansatz des Entfernens von Komponenten unter weiterer Vortäuschung ihrer Funktionalität können dabei Auswirkungen auftreten, die sich von den erzwungenen Verletzungen der IT-Sicherheit bis hin auf Folgen für Komfort und sogar Safety erstrecken. Daher werden im folgenden Kapitel 5 die wesentlichen Ursachen diskutiert und mögliche Lösungsansätze vorgestellt, bevor Kapitel 6 den Beitrag mit einer Zusammenfassung abschließt.

5 Abschließende Diskussion und Motivation von Gegenmaßnahmen

Das Hauptaugenmerkt dieses Beitrag lag bisher auf der praktische Untersuchung der Frage, welche Ergebnisse ein potenzieller Angreifer bei einer Attacke auf aktuelle automotive IT erzielen könnte, ohne dass ihm interne Herstellerdokumentation bereitgestellt werden. Nachdem die Ergebnisse des durchgeführten Black-Box Szenarios deutlich den Bedarf wirksamer, ganzheitlicher IT-Sicherheitsmaßnahmen im Automobil demonstrierten, soll in diesem abschließenden Kapitel zumindest kurz auf die zugrunde liegenden Ursachen und mögliche zukünftige Gegenmaßnahmen eingegangen werden. Auch wenn diese noch nicht im Fokus dieses Beitrages stehen, werden diese zukünftig verstärkt im Rahmen der weiteren Forschung behandelt (siehe Danksagungen).

Im Falle des Automobils sind im Gegensatz z.B. zum Heim-Computer tiefere Einblicke in und Konfigurationen an Systeminterna selbst ambitionierteren Nutzern praktisch nicht bzw. nur sehr eingeschränkt möglich. Diese Tatsache führt dazu, dass viele eingetretene Fehlerzustände (Safety-Verletzungen) durch den Besitzer im Wesentlichen nur symptomatisch erkannt werden können. Erst bei einem Besuch in der Werkstatt kann (z.B. über die herstellerspezifische Fahrzeugdiagnose-Lösung) eine genauere Fehleranalyse erfolgen und betroffene Teile ausgetauscht oder umkonfiguriert werden.
Diese Besonderheiten im gewohnten Umgang mit dem System Automobil können im Falle von gezielten Angriffen auf die IT-Sicherheit (Security-Verletzungen) jedoch fatale Auswirkungen haben. Schafft es ein Angreifer, das IT-System Automobil z.B. durch Einbringen eigenen schadhaften Programmcodes in eine seiner Komponenten zu infizieren, um ein bösartiges Ziel zu erreichen, so ist nicht damit zu rechnen, dass die gewohnten Maßnahmen zur Beseitigung eines solchen Fehlerzustandes auch hier greifen. Im Gegensatz zu mehr oder weniger zufällig aufgetretenen Fehlern wie Komponentenstörungen (Safety-Verletzungen), versucht ein Angreifer bei gezielt herbeigeführten IT-Security-Verletzungen, die für Anwender und System sichtbaren Auswirkungen in der Regel soweit wie möglich zu verbergen. Je nach Art der durch den Angriff verfolgten Absicht wird der Anwender keine ungewöhnlichen Symptome beobachten (oder hat beim plötzlichen Auftreten dieser keine Möglichkeit mehr einzuschreiten). Wie sich auch im praktischen Versuch gezeigt hat, müssen auch bei

einer routinemäßigen Fahrzeugdiagnose eines infizierten Fahrzeugs keine sichtbaren Anzeichen einer solchen, gezielt herbeigeführten, Manipulation des Fahrzeuges auftreten. Da die Fahrzeugdiagnose bis dato nur zum Aufdecken von nicht-absichtlichen Fehlerzuständen (Safety) dient, kann eingedrungener Schadcode (gezielte Angriffe auf die Security) die gelieferten Ergebnisse im Gegenteil sogar gezielt manipulieren. Wie anhand des Airbag-Beispiels gezeigt wurde, können neben der Verdeckung der Security-Verletzungen selbst auch Safety-kritische Systemmanipulationen vor dem Anwender (zunächst symptomlos) als auch vor Servicepersonal (Manipulation von Kfz-Diagnose) versteckt werden.

Identifizierung von Ursachen

Die zugrunde liegenden Ursachen für die vergleichsweise leichte Realisierbarkeit der demonstrierten Angriffe sind vielschichtig und beginnen bereits beim Design gegenwärtiger automotiver IT-Strukturen. Bemühungen, IT-Sicherheit im Automobil zu berücksichtigen, sind gegenwärtig nur punktuell erkennbar. Ein bekanntes Beispiel sind Wegfahrsperren, die bereits auf kryptographischen Protokollen basieren. Auch werden die Schnittstellen zum Einspielen von Flash-Updates (i.d.R. über das Diagnoseprotokoll) zunehmend kryptographisch abgesichert, um u.a. Integrität und Authentizität der eingespielten Betriebssoftware prüfen zu können (z.B. im Rahmen der Herstellerinitiative Software [HIS]). Allerdings sind die überwiegenden restlichen Teile des Gesamtsystems bislang kaum gegen gezielte Angriffe auf die IT-Sicherheit geschützt. Dies wurde im vorliegenden Beitrag beispielsweise anhand der Buskommunikation demonstriert, die zwischen den dezentral vernetzten Steuergeräten in der Regel völlig ungeschützt gegen gezielte Eingriffe abgewickelt wird. Dies wurde auch im vorliegenden Versuchsaufbau ausgenutzt, da im Falle des CAN Bus durch das Protokoll keine Möglichkeit zur Feststellung der Authentizität eingehender Nachrichten geboten wird. Dies erleichtert potenziellen Angreifern Angriffstechniken wie z.B. Spoofing-Attacken erheblich.

Identifikation von Schutzzielen und Motivation von Lösungsansätzen

Ein für den Einsatz im Automobil zugeschnittenes IT-Sicherheitskonzept sollte leisten, möglichst jede über Hard- oder Softwareeingriffe am oder im Fahrzeug vorgenommene Manipulation an den vernetzten Steuergeräten sowie ihrer Kommunikation erkennen und angemessen reagieren zu können. Als einige zentrale Schutzziele lassen sich beispielhaft folgende identifizieren:

- Die ***Integrität*** der einzelnen Steuergeräte angesichts gezielter Manipulationen sowohl in Bezug auf die aktive Betriebssoftware und die von ihr verwendeten Daten als auch in Bezug auf die Hardware des Geräts
- Die ***Authentizität*** von Nachrichten, die über die Kommunikationswege ausgetauscht werden
- Abhängig vom Inhalt der kommunizierten Daten die ***Vertraulichkeit*** der Übertragung von Nachrichten

Einige weitere Ziele wie z.B. das der ***Verfügbarkeit*** der Ressourcen (von Geräten bereitgestellte Dienste, Übertragungskapazität etc.) oder das der ***Integrität*** übertragener Nachrichten werden bereits auch aus Safety-Motivation heraus adressiert. Diese sollten jedoch mit Blick auf die Security (d.h. angesichts gezielter Angriffe) neu analysiert

werden. Beispielsweise genügen Prüfsummen wie CRC zum Erkennen von Integritätsverletzungen grundsätzlich nur den Anforderungen der Safety. Da ein Angreifer diese Werte ebenfalls kontrollieren kann, wären aus Sicht der Security zu einer wirksamen Absicherung beispielsweise digitale Signaturen erforderlich.
Maßnahmen zur Realisierung entsprechender Schutzmechanismen für das Automobil werden in der Forschung bereits diskutiert (vgl. z.B. [WWW]). Deutliches Potential zur Erkennung sowohl software- als auch hardwarebasierter Angriffe versprechen dabei auf kryptographischen Protokollen (insbesondere Public-Key-Kryptographie) basierende Ansätze. Für den Einsatz solches „Trusted Computing“ im Automobil werden jedoch verschiedenste besondere Anforderungen relevant, die individuell für diesen Einsatzzweck zu beachten sind. Dies beginnt bereits mit dem hohen Kostendruck in der Automobilproduktion und daraus resultierenden starken Ressourceneinschränkungen bis hin zu einer höheren Intensität zu erwartender *hardware*-basierter Angriffe auf Trusted-Computing-Elemente im Vergleich zu Desktop-PCs.
Angesichts der in Diskussion befindlichen Vernetzung zwischen Automobilen untereinander können darauf aufbauend weitere infrastrukturelle Sicherheitsarchitekturen notwendig werden. Hierunter fallen insbesondere adäquate Konzepte für netzübergreifende Public-Key-Infrastrukuren, über die z.B. für den Austausch besonders sensitiver Informationen eine Authentifizierung der i.d.R. zunächst unbekannten weiteren Verkehrsteilnehmer realisiert werden könnte.

6 Zusammenfassung

In diesem Beitrag haben wir zunächst auf die Bedrohung aktueller automotiver IT-Strukturen durch gezielte Angriffe auf die IT-Sicherheit hingewiesen. Dies konnte anhand eines praktischen Versuchsaufbaus mit gegenwärtig eingesetzter automotiver Hardware veranschaulicht werden, an der sich mit dem vorgestellten Ansatz des Vortäuschens von Komponentenfunktionalität beim Entfernen oder Deaktivieren von Komponenten ein komplexeres Angriffsszenario skizzieren ließ. Dies erfolgte anhand eines Airbagsystems, welches aus dem System entfernt wurde, jedoch nach wie vor angesichts der Fahrzeuganzeigen sowie sogar einer Fahrzeugdiagnose als vorhanden und fehlerfrei funktionierend erscheint. Anschließend wurden mögliche Folgen derartiger Angriffe auf Komfort und Safety des Automobils untersucht, die zugrunde liegenden Ursachen benannt und erste Ansätze für zukünftige Gegenmaßnahmen diskutiert.

7 Danksagungen

Diese Veröffentlichung entstand in Kooperation mit dem Verbundprojekt COmpetence in MObility (COMO, EU-Nr.: C-2007-5254). Der Inhalt dieser Veröffentlichung steht in alleiniger Verantwortung der Autoren und widerspiegelt somit in keiner Weise die Meinung der Europäischen Union.

Die Autoren möchten außerdem Herrn Stefan Kiltz für viele interessante Diskussionen zu automotiver IT-Sicherheit danken.

8 Literaturverzeichnis

[Kas05] Eugene Kaspersky: Viruses coming aboard? , Viruslist.com Weblog-Eintrag vom 24. 1. 2005, http://www.viruslist.com/en/weblog?discuss=158190454&return=1, Oktober 2007

[WWW] A.Weimerskirch, M.Wolf, T.Wollinger: "State of the Art: Embedding Security in Vehicles", In EURASIP Journal on Embedded Systems (EURASIP JES), Special Issue: Embedded Systems for Intelligent Vehicles, 2007

[GP06] Felix Gutbrodt, Michael Plewan: Schichtenarchitektur zur Realisierung von IT-Sicherheit für eingebettete Systeme, Automotive - Safety&Security 2006, 12.-13.Oktober 2006, Universität Stuttgart

[LDKH] Andreas Lang, Jana Dittmann, Stefan Kiltz, Tobias Hoppe; Future Perspectives: The Car and its IP-Address - A Potential Safety and Security Risk Assessment; In: Computer Safety, Reliability, and Security, Proceedings of the 26th International Conference SAFECOMP 2007, Nuremberg, Germany, September 2007; Springer LNCS 4680; pp. 40-53; Editors: Francesca Saglietti, Norbert Oster; ISBN 978-3-540-75100-7

[HD07] Tobias Hoppe, Jana Dittmann; Sniffing/Replay Attacks on CAN Buses: A Simulated Attack on the Electric Window Lift Classified using an Adapted CERT Taxonomy; In: Proceedings of the 2nd Workshop on Embedded Systems Security (WESS'2007), A Workshop of the IEEE/ACM EMSOFT'2007 and the Embedded Systems Week October 4, 2007

[CAN] BOSCH CAN, Webseite, www.can.bosch.com, Oktober 2007

[Vec07] Vector Informatik: CANoe; http://www.vector-worldwide.com/vi_canoe_de.html, Oktober 2007

[HL98] Howard, John D.; Longstaff, Thomas A.: A Common Language for Computer Security Incidents (SAND98-8667) / Sandia National Laboratories, 1998 (ISBN 0-201-63346-9)

[HKLD] Tobias Hoppe, Stefan Kiltz, Andreas Lang, Jana Dittmann; Exemplary Automotive Attack Scenarios: Trojan horses for Electronic Throttle Control System (ETC) and replay attacks on the power window system; In: Automotive Security - VDI-Berichte Nr. 2016, Proceedings of the 23. VDI/VW Gemeinschaftstagung Automotive Security, Wolfsburg, Germany; 27.-28. November 2007, VDI-Verlag, pp. 165-183, ISBN 978-3-18-092016-0, 2007

[HIS] HIS: Herstellerinitiative Software, http://www.automotive-his.de/. Version: 2007