Sichere Datenhaltung im Automobil am Beispiel eines Konzepts zur forensisch sicheren Datenspeicherung

Tobias Hoppe[1], Sönke Holthusen[2], Sven Tuchscheerer[1], Stefan Kiltz[1], Jana Dittmann[1]
[1] Arbeitsgruppe Multimedia and Security, Institut ITI, Fakultät für Informatik
[1,2] Otto-von-Guericke Universität Magdeburg
Universitätsplatz 2
39106 Magdeburg
{tobias.hoppe, sven.tuchscheerer, stefan.kiltz, jana.dittmann}@iti.cs.uni-magdeburg.de

Abstract: Seit mehreren Jahren wird in der Forschung auf potentielle Gefahren hingewiesen, die vorsätzliche Angriffe auf automotive IT-Systeme bergen [HKD08]. Aktuelle Arbeiten wie [Ko10] zeigen, dass Auswirkungen bis hin auf die leibliche Sicherheit (Safety) der Insassen zunehmend realistisch werden. Moderne automotive IT verarbeitet und speichert zunehmend auch personenbeziehbare Daten, so dass zusätzlich Beeinträchtigungen der Privatsphäre drohen. Folglich stellt die automotive IT-Sicherheit, d.h. der Schutz derartiger sensibler Daten vor unautorisiertem Ausspähen und Manipulationen ein wichtiges Forschungsziel dar. Diese Problematik adressierend, behandelt der vorliegende Beitrag Aspekte der sicheren Datenhaltung im Automobil. In diesem Beitrag wird ein kombiniertes Konzept zur sicheren Datenspeicherung vorgeschlagen und eine wissenschaftliche Diskussion angeregt. Es basiert auf dem bestehenden Konzept elektronischer Fahrzeugdatenschreiber, deren bisherige Lösungen jedoch meist primär zur Aufklärung *safety*-bezogener Ereignisse (insbesondere Verkehrsunfälle) konzipiert sind. Bedrohungen seitens der *Security* (z.B. Manipulationen von Daten im Gesamtfahrzeug) werden häufig nicht berücksichtigt. Der vorgestellte kombinierte Ansatz ist zusätzlich als strategische Vorbereitung für ggf. zukünftig folgende, IT-forensische Aufklärungen geeignet und adressiert somit auch Vorfälle, welche auf Verletzungen der Security zurückzuführen sind. Ziel ist, ein Konzept mit besonderem Fokus auf unterschiedliche Nutzer und deren variierende Sicherheitsanforderungen an die gesicherten Daten (wie Integrität, Authentizität und Vertraulichkeit) zu diskutieren.

1 Einführung / Motivation

Bei der Behandlung von Sicherheitsrisiken wird nicht nur im Automobilbereich zwischen zwei Ausprägungen der *Sicherheit* unterschieden. Ein sicherer Betrieb im Sinne der Funktionssicherheit (engl. *Safety*) berücksichtigt potentielle Komponentenausfälle oder auftretende Störungen und soll insbesondere die körperliche Unversehrtheit des Menschen bewahren. Die Informationssicherheit (IT *Security*) hat hingegen das Ziel, Vorkommnisse des unautorisierten Ausspähens und Manipulierens von Daten zu verhindern, erkennen bzw. behandeln zu können. Sie richtet sich damit gegen vorsätzliche Ereignisse und dient primär dem Schutz von Informationen.

Mit ihrem starken Einfluss auf die Unversehrtheit von Leib und Leben des Menschen sind moderne Automobile im Sinne der *Safety* bereits als sicherheitsrelevante Systeme

anerkannt. Die in Form vielzähliger Steuergeräte verbauten IT-Komponenten bieten bereits heute Möglichkeiten, ein Versagen sowie potentielle Fehlfunktionen verschiedenster automotiver (Teil-)Systeme erkennen zu können. Hierzu gehören beispielsweise digitale Fehlercodes (engl. DTC, Diagnostic Trouble Codes), die sich ein Steuergerät nach Detektion eines auffälligen Zustandes vermerkt und die anschließend (z.B. in der Werkstatt im Rahmen der regelmäßigen Inspektion) über die Diagnoseschnittstelle ausgelesen und zur Ursachenanalyse herangezogen werden können. Fehlercodes werden meist bei Ereignissen generiert, die im Vorfeld durch die Entwickler als potentielle Fehlzustände definiert wurden und sind damit hauptsächlich für ungewünschte Vorkommnisse konzipiert, die zufällig, sporadisch oder systematisch auftreten können.

Im Rahmen der seit jeher betriebenen vorsätzlichen Manipulationen an Fahrzeugsystemen werden zunehmend auch Veränderungen ihres Datenstandes betrieben. Derartige Verletzungen der *Security* können durch die bisherigen Einrichtungen zur Fehlzustandserkennung aktuell jedoch nicht bzw. nur sehr eingeschränkt erkannt werden (z.B. weil vorsätzliche Eingriffe nicht als relevante Ereignisse definiert wurden oder vorhandene Prüfbedingungen durch gezielte Manipulationen nicht verletzt werden). Gerade im Fall des safety-relevanten Automobils kann der Nachweis vorsätzlicher, unautorisierter Eingriffe von essentieller Bedeutung sein, wie auch Literatur aus dem Bereich der Unfallforschung und –rekonstruktion unterstreicht: *„Für den Sachverständigen ist es wichtig zu erkennen, ob an dem von ihm zu untersuchenden Fahrzeug bzw. Steuergerät Tuningmaßnahmen vorgenommen wurden."* ([BM09], S. 826). Während Tuning-Maßnahmen (vgl. auch [Bo08], Kapitel „Selbstbau und Tuning") im Automobilbereich eines der bekanntesten Felder teils unautorisierter Manipulationen darstellen, zeichnen sich weitere, modernere Ausprägungen IT-basierter Angriffe auf automotive Systeme ab. Einige Beispiele aus Forschung und Praxis sind das Vortäuschen der korrekten Funktion defekter oder entfernter Airbags [HKD08], das Senden gefälschter Verkehrsinformationen [BD07], unautorisierte (De-)Aktivierung der Bremsen [Ko10] oder das aus dem Internet initiierte, unberechtigte Lahmlegen einer gesamten Fahrzeugflotte per Funk [MFA10].

1.1 Forschungsziel und Stand der Technik

Ein wichtiges Forschungsziel stellt daher dar, in Zukunft auch die Aufklärung derartiger vorsätzlicher Eingriffe zu fördern. Als ein Beispiel finden sich in bestehenden Arbeiten bereits Untersuchungen zur Anpassung von Intrusion Detection Systemen (IDS) auf die automotive Domäne, um Angriffe auf automotive IT zunächst erkennen (vgl. [HKD09, MHD10]) und potentiell schwerwiegende Folgen einschränken zu können.

In Fokus dieses Beitrags steht die sichere Protokollierung / Speicherung fahrzeuginterner Daten um im Fall potentieller Vorfälle ggf. folgende IT-forensische Untersuchungen und damit deren Aufklärung erheblich unterstützen zu können. Derartige, vorab eingerichtete prophylaktische Vorkehrungen für IT-basierte Systeme (hier: das Fahrzeug) werden im Prozessmodell zur IT-Forensik nach [KHA09] auch als strategische Vorbereitung bezeichnet. Doch auch abseits der IT-Forensik gibt es sinnvolle Anwendungen für ein entsprechendes Datensicherungssystem. Ausgewählte Beispiele und jeweils relevante Anforderungen/Schutzziele an die Datenspeicherung werden in der Folge mit identifi-

ziert und einbezogen. Basierend auf Ergebnissen aus [Ho10] und ergänzt durch zusätzliche Betrachtungen wird in diesem Beitrag ein entsprechend erweitertes Konzept für ein solches System vorgeschlagen und diskutiert, das im weiteren Verlauf des Beitrags als „Forensischer Fahrzeugdatenschreiber“ (FFDS) bezeichnet wird.

Im Kontext einer prophylaktischen, automotiven Datenprotokollierung ist als Stand der Technik insbesondere auf das bestehende Konzept des Unfalldatenschreibers (UDS) zu verweisen. Für den speziellen Anwendungsfall der Unterstützung einer Unfallrekonstruktion speichert ein UDS ausgewählte Informationen (z.B. Geschwindigkeiten, Längs-/Querbeschleunigungen, Blinker-/Bremsvorgänge) i.d.R. nur für ein kurzes Zeitfenster; laut [BM09] genügen in der Regel z.B. ca. 45 Sekunden, um eine erhebliche Erleichterung bei der Unfallrekonstruktion zu erzielen. Entsprechende Produkte sind bereits seit mehreren Jahren verfügbar (z.B. Verweise in [Ha03]). Auch trotz Standardisierungsbemühungen in verschiedenen Ländern (z.B. bzgl. der Bereitstellung aufgezeichneter Daten [EDR06]) konnten sich UDS bisher nicht im breiten Einsatz durchsetzen.

Dieser Beitrag gliedert sich wie folgt: Im folgenden Abschnitt 2 werden fünf exemplarische Rollen von Nutzern eines entsprechenden Systems vorgestellt und ihre Anforderungen an die Datensicherung diskutiert. Ein Vorschlag für ein entsprechendes Konzept wird in Abschnitt 3 vorgestellt und in Abschnitt 4 anhand der prototypischen Umsetzung und ausgewählten Beispielen illustriert. Eine Diskussion zur Erfüllung der Anforderungen und ausgewählter Vor- und Nachteile folgt in Abschnitt 5, bevor eine Zusammenfassung und ein Ausblick in Abschnitt 6 diesen Beitrag schließt.

2 Ausgewählte Anwendungsfälle und ihre Anforderungen

Bzgl. der durch das FFDS vorgenommenen Datensicherung aus Fahrzeugen stehen im Kontext dieses Beitrags primär digitale Daten im Fokus, die intern über Feldbustechnologien wie CAN, LIN, MOST oder FlexRay [ZS08] ausgetauscht werden. Eine regelmäßige Protokollierung ausgewählter Daten kann zu unterschiedlichen Anwendungszwecken relevant sein. Dieser Abschnitt stellt fünf beispielhafte Rollen vor und diskutiert deren Anforderungen hinsichtlich des Schutzbedarfs der zu speichernden Logdaten.

2.1 Exemplarische Rollen

Rolle R1 — Fahrzeugbesitzer: Bereits für den Besitzer selbst, der oft der hauptsächliche Nutzer des Fahrzeuges ist, bieten sich sinnvolle Anwendungszwecke für ein entsprechendes Logging-System, etwa zur Erstellung eines digitalen Fahrtenbuchs oder Statistiken zu seiner Fahrweise, z.B. um Kosten und Schadstoffemissionen zu minimieren. Auch kann er die geloggten Daten als (entlastendes) Beweismaterial nutzen wollen – z.B. im Falle ihm vorgeworfener Verkehrsdelikte oder um (auch in anderweitigen Streitfällen) die (Nicht-)Nutzung des Fahrzeug zum fraglichen Zeitpunkt belegen zu können.

Rolle R2 — Versicherung: Versicherungen bieten zunehmend flexiblere Tarifmodelle, die Fahrgewohnheiten und –verhalten mit einbeziehen (z.B. bzgl. Wegstrecken, Ge-

schwindigkeiten, Fahrtzeiten oder Lokalitäten), wozu entsprechende Daten für die Versicherung zu protokollieren sind. Als eine frühe Realisierung dieses „Pay as you drive" Prinzips sieht z.B. das System MyRate [MR10] ein an der On-Board-Diagnose (OBD) Schnittstelle platziertes Gerät zur Protokollierung vor.

Rolle R3 — Unfallrekonstruktion: Die teils nach Verkehrsunfällen durchgeführte Unfallrekonstruktion hat das Ziel, u.a. anhand des Spurenbildes den Unfallablauf möglichst genau rekonstruieren zu können, insbesondere zur Klärung von Schuldfragen. Auch Daten aus den beteiligten Fahrzeugen können hierzu wertvoll sein. Zusätzlich zu den Leistungsmerkmalen eines UDS (Abschnitt 1.1) kann ein FFDS diese Aufgabe ebenso erfüllen und dem Sachverständigen noch zusätzlichen Nutzen bieten (z.B. Zugriff auf die Vorgeschichte des Fahrzeuges).

Rolle R4 — IT-Forensiker: Insbesondere auch angesichts zukünftiger Funkkommunikation zwischen Fahrzeugen sowie zur Infrastruktur könnten gezielte Angriffe auf automotive IT auch von externer Seite weiter zunehmen (vgl. auch [Ko10]), die teils einer nachträglichen Aufklärung nach Prinzipien der IT-Forensik [KH02] bedürfen. Eine erhebliche Unterstützung des IT-Forensikers kann hierbei insbesondere durch eine prophylaktische, forensik-konforme Protokollierung derartiger Daten geboten werden (vgl. Abschnitt 1.1), die auf das Eindringen eines Angreifers hinweisen können oder durch ihn potentiell ausgeführte Aktionen aufzeigen. Dies kann z.B. Zeit und Kontext etablierter Verbindungen (z.B. Diagnose oder Funk) oder die Ansteuerung ausgewählter Aktoren umfassen. Auch zur Laufzeit nicht näher spezifizierbare Anomalien können als potentielle Anzeichen security-relevanter Aktivitäten vorsorglich gesichert werden.

Rolle R5 — Werkstatt: Ergänzend zu bestehenden Fehlercodes (s. Abschnitt 1) können regelmäßig protokollierte Informationen und Anomalien auch Werkstätten bei der Ursachenanalyse rein safety-bezogener Störungen unterstützen. Während Fehlercodes oft nur Ort, Zeitpunkt und Art eines auffälligen Zustandes vermerken, kann in den Logdaten gezielt nach zeitlich und kausal korrelierenden Ereignissen gesucht werden. Dies kann die Behebung von Mängeln beschleunigen und so auch zu einer Kostenersparnis führen.

2.2 Sicherheitsanforderungen an das FFDS bzgl. der vorgestellten Anwendungsfälle

Die Diskussion der Sicherheitsanforderungen erfolgt in diesem Teilabschnitt exemplarisch für die Schutzziele Authentizität, Integrität und Vertraulichkeit. Die Betrachtungen erfolgen zusammenfassend für die internen (Besitzer/Nutzer des Fahrzeuges; R1) und externen Nutzer (dritte Parteien; R2-R5) des FFDS, da diese jeweils in ihren wesentlichen Anforderungen hinsichtlich des Schutzes der gesicherten Daten übereinstimmen.

Zunächst ist festzustellen, dass die Sicherheitseigenschaften des FFDS auch für den Fahrzeugbesitzer (bzw. die Nutzer des Fahrzeuges) von großer Bedeutung sind - z.B. gegenüber einem alternativ denkbaren ungeschützten Logging: Angesichts des großen Anteils personenbezogener und –beziehbarer Daten in aktuellen Automobilen kann als primäre Sicherheitsanforderung des Besitzers die Vertraulichkeit der gespeicherten Daten angesehen werden. Diese sollten daher gegen das Auslesen durch unberechtigte Personen geschützt sein. Als sekundäre Anforderungen seinerseits können die Integrität und

die Authentizität der Logdaten hinzu kommen, wenn er im Einzelfall die Möglichkeit haben will, für ihn gespeicherte Daten als Beweismaterial einsetzen zu können.

Für die externen Parteien sind die Integrität und Authentizität der Logdaten als primäre Anforderung zu sehen: Zum verlässlichen Durchführen ihrer Aufgabe (d.h. zur Ermittlung der Versicherungsbeträge, Rekonstruktion von Unfällen und IT-Vorfällen sowie zur Fehlersuche) dürfen diese Daten weder durch Nutzer oder Dritte verfälscht worden sein, noch sollten integre Daten aus einem anderen Fahrzeug/FFDS unerkannt eingebracht werden können. Im Falle des IT-Forensikers leiten sich beide Schutzziele direkt aus den forensischen Prinzipien ab [KH02]. Die Vertraulichkeit der Logdaten ist für die Aufgabe der externen Rollen i.d.R. nicht von Bedeutung; deren Interesse an einer Wahrung kann als maximal sekundär eingeschätzt werden (ggf. bestehen jedoch gesetzliche Vorgaben).

Nutzergruppe	Primäre Schutzziele	Sekundäre Schutzziele	Wesentliche Kategorien potentiell zu erwartender Angriffe / Angreifer
Intern (R1)	Vertraulichkeit	Integrität, Authentizität	Einsehen der Daten durch unberechtigte Dritte
Extern (R2-R5)	Integrität, Authentizität	Vertraulichkeit	R2-R3: Manipulation durch interne Nutzer R2-R5: Manipulation durch unberechtigte Dritte

Tabelle 1: Übersicht über relevante Beispiele für gestellte Schutzziele und erwartete Angreifer

Die zuvor erfolgten Abschätzungen zur Relevanz der betrachteten Schutzziele aus Sicht der vorgestellten Rollen werden in Tabelle 1 gegenübergestellt. Letztendlich sind die bei einer Realisierung des FFDS zu beachtenden Schutzziele jedoch im Kontext des Gesamtsystems zu sehen: Beispielsweise ist die Anforderung des Besitzers/R1 an die vertrauliche Speicherung auch auf Datensätze anzuwenden, die für Nutzer anderer Rollen (z.B. die Werkstatt/R5) gespeichert werden – auch wenn diese Anforderung aus deren Sicht nicht relevant ist. Folglich sollte die Vertraulichkeit, Integrität und Authentizität protokollierter Daten durch einen FFDS gleichermaßen durchgängig gesichert werden.

3 Konzept

Das vorgeschlagene Konzept für den FFDS, das den folgenden Betrachtungen zugrunde liegt, ist in der folgenden Abbildung 1 skizziert. Es ist so gestaltet, dass es bereits auf ein heutiges automotives System anwendbar ist, ohne dass dieses anwendungsspezifische Anforderungen erfüllen muss. Dazu wird dem Fahrzeug ein zusätzliches Gerät (mittlerer Block in Abbildung 1) hinzugefügt, das zwecks lesenden Zugriffs an dessen interne Busnetzwerke (linker Teil in Abbildung 1) angeschlossen wird. Busnachrichten aus allen relevanten Teilnetzwerken, die ggf. auch unterschiedliche Feldbustechnologien verwenden, werden von einem *BusListener* entgegengenommen und mit dem Zeitstempel des Eingangs versehen. Zur weiteren, parallelen Bearbeitung werden sie anschließend an zwei Komponenten weitergereicht: Der *Filter* hat die Aufgabe, nach einem festen Regelwerk (anhand rollenindividueller Filterregeln, siehe Abschnitt 4) die für jeden auf dem FFDS registrierten Nutzer relevanten Informationen zur Speicherung zu selektieren (bzw. irrelevante auszublenden). Der *Detektor* untersucht die aktuelle Kommunikation parallel auf Anomalien, die sich allein auf Basis der statischen Filterregeln nicht abdecken lassen (z.B. in Form eines automotiven IDS / siehe Abschnitt 1.1). Dies kann z.B.

die Detektion von Angriffsmustern (vgl. [HKD09]) sowie auch allgemeine Auffälligkeiten umfassen, die für einige Rollen ebenfalls relevant sein können – z.B. ein Aussetzen der Stromversorgung, das potentiell auf einen Versuch des Verschleierns einer Manipulation hinweist. In solchen Fällen kann zudem auch der aktuelle Loglevel erhöht werden.

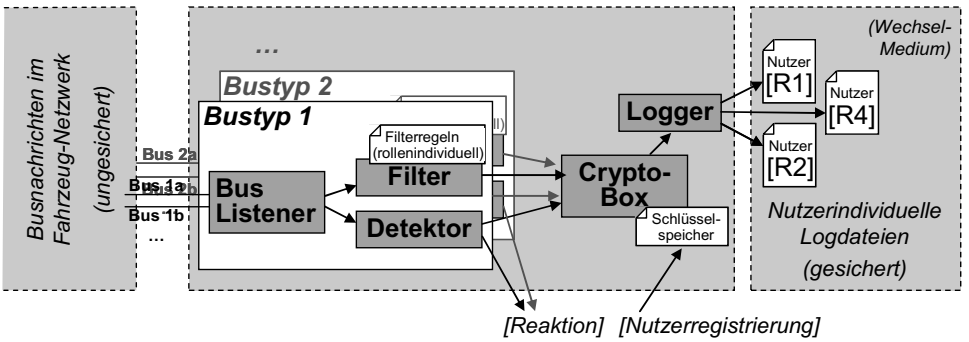

Abbildung 1: Vorgeschlagenes Konzept des forensischen Fahrzeugdatenschreibers (FFDS)

Die zur Speicherung selektierten Nachrichten und Ereignisse werden anschließend von der *CryptoBox* kryptographisch gesichert, um sie danach unter Einhaltung der geforderten Schutzziele (vgl. Abschnitt 2) durch den *Logger* in nutzerindividuellen Logdateien auf einem Wechseldatenträger (z.B. SD-Karte) ablegen zu können.

3.1 Das zugrundeliegende kryptographische Konzept

Zur Einhaltung der geforderten Sicherheitseigenschaften ist das kryptographische Konzept entscheidend, das seitens des FFDS in der CryptoBox zu implementieren ist.

Zur Sicherstellung der Vertraulichkeit der gesicherten Daten sieht das Konzept die Verschlüsselung der zu sichernden Einträge vor, um unbefugte Einsicht möglichst einzuschränken. Hierzu nutzt das Konzept die Vorteile asymmetrischer Verschlüsselungsverfahren: Bei der Registrierung eines neuen Nutzers wird sein Public Key im Schlüsselspeicher des FFDS hinterlegt, mit dem der FFDS jederzeit Daten verschlüsselt in der Logdatei des Nutzers ablegen kann. Um den Ressourcenbedarf gering zu halten (sowohl bzgl. Rechenleistung als auch Speicherplatz für die Chiffrate) kommt hierbei ein hybrides Verfahren zum Einsatz, bei der die Logeinträge über ein symmetrisches Verschlüsselungsverfahren chiffriert werden und lediglich die hierzu verwendeten, regelmäßig wechselnden Session-Keys asymmetrisch verschlüsselt mit abgelegt werden [Bu10].

Der FFDS hat die Authentizität und Integrität der Logdaten zusätzlich zu sichern, denn sonst könnte z.B. der Fahrzeugbesitzer mit dem Public Key der Versicherung Logdateien mit beliebigen verschlüsselten Inhalten auch außerhalb des FFDS selbst erzeugen. Die Versicherung muss daher überprüfen können, ob die z.B. jährlich bereitgestellten Logdateien wirklich durch den angemeldeten FFDS generiert wurden sowie unverfälscht sind. Dazu wird für jeden FFDS zusätzlich ein eigenes asymmetrisches Schlüsselpaar generiert. Der Private Key muss dazu sicher im Schlüsselspeicher innerhalb des FFDS verwahrt werden (dieser kann z.B. als Smartcard realisiert sein) und wird zum Signieren der

generierten Logeinträge verwendet (was ebenfalls blockweise erfolgt). Die Zugehörigkeit des entsprechenden Public Keys zu seinem FFDS wird dem Fahrzeugbesitzer durch den Hersteller des FFDS auf einem Zertifikat bescheinigt. Über dieses kann er z.B. der Versicherung, die er als Nutzer auf seinem FFDS registrieren möchte, den Public Key des FFDS nachweisbar für spätere Integritäts- und Authentizitätsprüfungen überlassen.

Soll der FFDS zusätzlich die Authentizität von Nutzern überprüfen können, die sich in einer unterstützten Rolle zum Aufzeichnen von Fahrzeugdaten anmelden, kann dies über eine vertrauenswürdige, dritte Instanz erfolgen. Als ein Beispiel möchte sich am FFDS ein neuer Nutzer in der Rolle ‚Versicherung' anmelden. Neben seinem Public Key muss er dann auch ein Zertifikat vorweisen, in der eine übergeordnete Instanz bescheinigt, dass es sich bei ihm um eine zugelassene Versicherung handelt. Der FFDS müsste für die Verifikation mit dem Public Key dieser Instanz ausgestattet sein, bei der es sich in einem einfachen Fall um den Hersteller des FFDS handeln kann. Äquivalent ließe sich über Sperrzertifikate auch ein Revocation-Management umsetzen (z.B. über zukünftige Car-to-Infrastructure Kommunikation).

Eine exemplarische Umsetzung des Konzeptes sowie eine detailliertere Diskussion bzgl. ausgewählter Vor- und Nachteile stehen im Fokus der folgenden Abschnitte 4 und 5.

4 Exemplarische Umsetzung und Illustration

Im Rahmen von [Ho10] wurde ein erster Prototyp als exemplarische Umsetzung des Konzeptes implementiert. Diese verwendet das Bussystem Controller Area Network (CAN), da es im Automobilbereich die zurzeit am häufigsten eingesetzte Feldbus-Technologie darstellt [ZS08]. Aus Anwendersicht besteht eine CAN-Botschaft im Wesentlichen aus einer numerischen ID (sog. CAN-ID), die gleichzeitig den Typ der Nachricht sowie ihre Priorität repräsentiert, sowie zwischen 0 und 8 Bytes an Nutzdaten. In den Nutzdaten werden i.d.R. mehrere Informationen, sog. Signale, gebündelt. Abbildung 2 illustriert den Aufbau der Nutzdaten einer fiktiven CAN-Botschaft (CAN-ID 0x3B7, 3 Nutzdatenbytes `A3 C1 53`), über die Signale zur Anzeige an das Kombiinstrument gesendet werden. In diesem Beispiel sind dies die aktuelle Geschwindigkeit (8 Bit) sowie je ein 1-Bit-Flag zum Setzen der Airbagwarnleuchte und zum Signalisieren eines eingehenden Anrufs. Ist die Rufnummer des Anrufers im Telefonbuch gespeichert, wird in letzterem Fall zusätzlich eine Kennung zur Anzeige seines Namens angegeben.

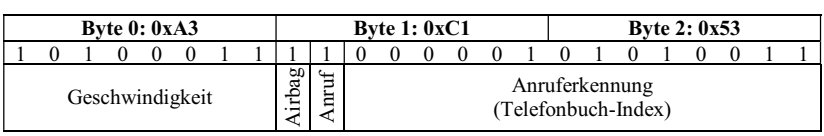

Abbildung 2: Aufteilung der Nutzdaten einer fiktiven CAN-Botschaft des Typs 0x3B7

Wie zuvor anmotiviert, benötigen verschiedene Rollen für ihre Zwecke nur einen Teil der kommunizierten Informationen und sollten nur entsprechende Zugriffe erhalten (Prinzip des notwendigen Wissens, vgl. [Eck03]). Am Beispiel der Busnachrichten o.g. Typs liefert Tabelle 2 eine exemplarische Zuordnung der enthaltenen Signale für die

Rollen Besitzer (R1), Werkstatt (R5) und Versicherung (R2, für die restlichen Rollen aus Abschnitt 2 ließe sich dies äquivalent vornehmen). Beispielsweise sollten sensible Daten wie Anruferkennungen (personenbeziehbare Daten auf Dritte) im Falle des Loggens nur einem begrenzten Personenkreis (im Wesentlichen dem Fahrzeugnutzer selbst) zugänglich sein. Während für Versicherungen z.B. bei Schadensfällen die Tatsache eines Anrufs als anonyme, binäre Information von Interesse sein kann, sollten für eine Werkstatt beide Angaben irrelevant sein. Dies wird durch den Filter (s.u. und Abb. 1) berücksichtigt. Damit der Vertraulichkeitsgewinn durch die rollenindividuelle Filterung für den Fahrzeugbesitzer transparent ist, muss der verwendete Regelsatz öffentlich sein.

	Besitzer (R1)	**Werkstatt (R5)**	**Versicherung (R2)**	**…**
Aktuelle Geschwindigkeit	X	X	X	…
Ereignis: Fehlfunktion Airbagsystem	X	X	-	…
Ereignis: eingehender Anruf	X	-	X	…
Anruferkennung (Telefonbuch-Index)	X	-	-	…

Tabelle 2: Beispiele für relevante Informationen einzelner Rollen (bzgl. CAN-Nachricht 0x3B7).

Aufgrund der bereits vorhandenen Unterstützung des CAN Protokolls erfolgt die Implementierung zunächst als C++ Programm unter Linux. Der ***BusListener*** für die gewählte Feldbustechnologie CAN verwendet die im Linux-Kernel zur Verfügung stehende SocketCAN Schnittstelle[1] und gibt die empfangenen Pakete samt Zeitstempel und Kennung des Eingangskanals zur weiteren Bearbeitung weiter. Der ***Filter*** wendet auf diese gemäß dem o.g. Prinzip rollenindividuelle Filterregeln an. Diese enthalten für jeden zu sichernden Nachrichtentyp eine Bitmaske, die alle bis auf die relevanten Bits ausblendet (Verknüpfung über logisches Und). Laut Tabelle 2 besteht z.B. für die Rolle Werkstatt (R5) z.B. eine Filterregel für die CAN-ID *0x3B7* mit der Filtermaske *FF 80 00* (Bits: *11111111 10000000 00000000*), die die Nutzbytes *A3 C1 53* der CAN-Nachricht aus Abbildung 2 zu *A3 80 00* filtert (Bits: *10100011 10000000 0000000*). Als zu sichernder Logeintrag wird jeweils eine Klartextzeile erstellt, die den Zeitstempel und Kanal des Eingangs, die CAN-ID und die gefilterten Inhalte umfasst (vgl. Abbildung 3). Bei der Implementierung der ***CryptoBox*** wurde die Bibliothek Botan[2] genutzt. Von den durch sie bereitgestellten kryptographischen Algorithmen wurden für die Umsetzung des Konzepts exemplarisch die aktuell als sicher eingestuften Verfahren AES-256 (symmetrisch), RSA-4096 (asymmetrisch) sowie SHA-256 (Hashfunktion) gewählt (vgl. auch [Bu10]). Die Verschlüsselung folgt dem im Abschnitt 3 vorgestellten Konzept. Da die (hier auf geloggten und gefilterten CAN-Nachrichten basierenden) Protokolleinträge blockorientiert sind, erfolgt die symmetrische AES-Verschlüsselung als Blockchiffre im CBC Modus (Cipher Block Chaining). Dies erschwert einerseits Offline-Angriffe auf die verschlüsselten Daten (im ECB Modus (Electronic Code Book) werden gleiche Klartextblöcke grundsätzlich als identische Chiffreblöcke abgelegt) und ist andererseits ein guter Kompromiss hinsichtlich der Performanz (im Vergleich zum OFB und CFB Modus, vgl. auch [Bu10]). Die von der CryptoBox gesicherten Logeinträge werden abschließend durch den ***Logger*** in den nutzerindividuellen Logdateien abgelegt. Wie Ab-

[1] siehe http://developer.berlios.de/projects/socketcan/
[2] siehe http://botan.randombit.net/

bildung 4 illustriert, wurde für diese ebenfalls ein Textformat gewählt, bei der zeilenweise ein Header den Typ des Eintrags anzeigt und die verschlüsselten Nutzdaten in Base-64-Kodierung[3] folgen. Entsprechend des in Abschnitt 3 beschriebenen Konzepts wird ein neuer, verschlüsselter Session-Key in einer `::key::` Zeile abgelegt. Nach dessen Entschlüsselung mit seinem Private Key kann der zugehörige Nutzer alle bis zum nächsten Schlüsselwechsel folgenden Logeinträge (`::mes::`) und Signaturen (Zeile `::sig::`) entschlüsseln. Äquivalent ermöglichen ihm die Signaturen, jeweils einen Block von Nachrichten auf Integrität und Authentizität zu überprüfen

```
1269618569.529082:can1:3B7:3:A38000
1269618569.529313:can2:420:8:00F273A3B42D0000
                          (…)
```

Abbildung 3: Schematischer Aufbau gefilterter CAN-Nachrichten als Logeintrag (z.B. für R5)

```
::key::5temeDmAUg6Rrq86sMyWViakoTnI40Jf2OVEc2hbpVKgRxRWel0iQ4Fq/dGgbNsR...
::mes::XCB2yafgPK0Tc2FeU2FcgZ67oHSm6XmtIOaYJnbGbBUEpSJz8+6aFgK+doHFQc83
::mes::YdjrOJJ0wvKQan9/4a7tBZ1c6o5Te+dRmjae+oBQSxt3XyXmJNsnnDVbtIdlcy0w
                                    (…)
::sig::kJD4ptmphyP6HCwTc9U8muEn0DEYUhYJhZSrRHSZ9Y3IwZ2mQEVHwj9GGYWh/DjD...
::key::(…)                          (…)
```

Abbildung 4: Schematischer Aufbau der gesicherten Logdateien (z.B. für einen Nutzer aus R5)

Da der Fokus auf die Filterung und Sicherung der Logdaten liegt, ist der ***Detektor*** im vorliegenden Prototyp lediglich rudimentär umgesetzt. Er kann in Zukunft jedoch z.B. um die in [HKD09] umgesetzten IDS-Konzepte ergänzt werden.

5 Diskussion des Konzeptes und der Umsetzung

In diesem Abschnitt werden abschließend ausgewählte Vor- und Nachteile diskutiert, die das vorgeschlagene Konzept (sowie die aktuelle Umsetzung) auszeichnen.

Schlüsselmanagement und Registrierung: Als eine zentrale Eigenschaft des Konzepts muss jeder Nutzer bereits im Vorfeld mit seinem Public Key auf dem FFDS registriert werden. Während die Versicherung (R2) und Stammwerkstatt (R5) im Vorfeld i.d.R. bekannt sind, kann dies im Fall anderer externer Rollen ggf. ein Problem darstellen. Da ein konkreter Unfallrekonstrukteur oder IT-Forensiker i.d.R. erst im Fall eines Vorkommnisses zugewiesen wird, können hier im Vorfeld keine individuellen Schlüssel hinterlegt werden. Eine Möglichkeit ist, für diese Rollen ein globales Schlüsselpaar einzusetzen, das seitens der zugehörigen Vereinigung verwaltet wird (potentiellen Vertraulichkeitsrisiken kann durch ausreichend restriktive Filterregeln für diese Rollen vorgebeugt werden). Als Alternative/Kompromiss kann der Besitzer vorab virtuelle Nutzer dieser Rollen anmelden, die Private Keys verwahren und beim Eintreten des jeweiligen Falles an den Ausführenden übergeben. Auch ist eine Erweiterung des Konzepts um Verfahren zum Widerrufen (z.B. wie in Abschnitt 3.1 kurz skizziert) und Updaten eingesetzter Schlüssel notwendig. Dies steht als Teil zukünftiger Arbeiten zur Diskussion.

[3] siehe RFC4648; http://tools.ietf.org/html/rfc4648

Berücksichtigte Schutzziele: Die Adressierung der *Vertraulichkeit* der gesicherten Daten ist ein wesentlicher Vorteil des Konzepts: Selbst wenn ein Angreifer an sämtliche im FFDS enthaltenen Informationen (inkl. kryptographischer Schlüssel) gelangt, ist es ihm nicht möglich, vorhandene (d.h. vor dem Einbruch generierte) Logeinträge zu entschlüsseln (allenfalls mit Ausnahme solcher Einträge, für die noch der aktuelle Session-Key gilt). Hierfür benötigt er die geheimen Schlüssel der Nutzer, die zu keiner Zeit auf dem System vorgehalten werden. Als Nachteil kann dagegen angesehen werden, dass der FFDS für die Signierungsvorgänge (Sicherung der *Authentizität und Integrität* der Logdaten) mit einem eigenen Private Key auszustatten ist: Gelangt ein Angreifer an diesen, kann er (zusammen mit den Public Keys der Nutzer) beliebige signierte Logdateien erzeugen (ein selektives Verfälschen bestehender Inhalte gestaltet sich mangels Möglichkeit der Entschlüsselung jedoch schwierig, s.o.). Dies macht den Einsatz von vergleichsweise teurerem, sicherem Speicher (z.B. einer Smartcard) erforderlich, um die benötigten Geheimnisse sicher im FFDS hinterlegen zu können. Im Falle einer sicheren Implementierung ist als wesentlicher Angriff auf die gesicherten Daten das Unbrauchbarmachen (z.B. Löschen/Überschreiben) der Logdateien zu nennen. Gezielte Angriffe auf die gesicherten Datenbestände sind problematisch: z.B. kann blockweises Löschen oder Vertauschen von Einträgen anhand der enthaltenen Zeitstempel (siehe Abb. 3) erkannt werden; eine Erweiterung um Sequenznummern ist zudem möglich.

Sicherheit kryptographischer Verfahren: Zukünftig könnten Angriffe auf die eingesetzten kryptographischen Verfahren effektiver werden. Gelangt ein Angreifer beispielsweise über Known-Plaintext-Angriffe [Bu10] an die symmetrischen Schlüssel oder durch Faktorisierung [Bu10] von RSA Public Keys an die Private Keys der registrierten Nutzer, könnten die geforderten Schutzziele nicht mehr gewährleistet werden. Während der Lebenszyklus kryptographischer Verfahren aktuell deutlich unter dem Lebenszyklus moderner Automobile liegt (oft 15-20 Jahre), kann sich z.B. ein nachträglicher Wechsel der kryptographischen Algorithmen aufgrund der eingeschränkten Systemressourcen schwierig gestalten. Potential bietet hier z.B. speziell auf eingebettete (automotive) Systeme zugeschnittene *light-weight* Kryptographie (vgl. www.ecrypt.eu.org/lightweight/).

Authentizität und Integrität der Eingangsdaten: Heutige automotive Busnetzwerke bieten noch keine Schutzmechanismen, die den Anforderungen der IT-Security genügen (z.B. für Authentizitäts- und verlässliche Integritätsprüfungen). Auf heutige Fahrzeuge angewandt, kann der FFDS die beschriebenen Schutzziele der zu protokollierenden Daten erst ab deren Eingang gewährleisten. Bereits an den Eingangsdaten erfolgte Manipulationen können daher heute noch nicht abgedeckt werden, d.h. ein Angreifer könnte das System nach physischem Umlegen der Eingangskanäle z.B. mit simulierten oder gezielt gefilterten Eingabedaten versorgen. Der Nachweis einer solchen Manipulation an einem heutigen System wäre symptomatisch anhand der gesicherten Logdaten zu führen (z.B. durch Auffinden von Widersprüchen in korrelierten Daten). Mittelfristig könnten Authentifizierungs-Mechanismen auf Geräteebene (z.B. durch Entwicklungen wie in [BZ08]) mit einbezogen werden, um die Echtheit der an der Kommunikation beteiligten Geräte festzustellen. Langfristig kann diese Lücke z.B. durch zukünftige Security-Erweiterungen automotiver Bussysteme effektiver geschlossen werden. Entsprechende Konzepte werden aktuell erforscht (z.B. [We09]), um potentiellen zukünftigen Bedrohungen wie den in [Ko10] demonstrierten begegnen zu können.

Erweiterungspotential: Das vorgeschlagene erste Konzept ist noch bzgl. weiterer Aspekte zu erweitern. Beispielsweise sollte zur beweiskräftigen Verwertung der Logdaten ein besonderes Augenmerk auf die Zeitsynchronität gesetzt werden. Ein weiterer Punkt ist, dass je nach Anzahl der registrierten Nutzer und Umfang der zu sichernden Daten sowie auch angesichts potentieller Denial of Service (DoS) Angriffe Kapazitätsengpässe seitens des Speichermediums auftreten können. Hier bietet es sich an, den Logger (siehe Abb. 1) mit robusten Verdrängungsstrategien auszustatten, wozu ein prioritätsbasierter Ansatz vorgeschlagen wird: Einzelne Rollen wie die Versicherung haben einen besonderen Anspruch auf die Vollständigkeit einiger Daten, während andere Daten bei Kapazitätsengpässen eher überschrieben werden können. Als eine Alternative zur nahe liegenden Zuordnung der gesicherten Einträge zu Prioritätsklassen kann die Erweiterung des kryptographischen Konzepts um homomorphe Algorithmen geprüft werden, die eine Suche auch auf den verschlüsselten Datenbeständen erlauben.

6 Zusammenfassung / Ausblick

In diesem Beitrag wurde ein Konzept vorgestellt, wie Informationen aus automotiven IT-Systemverbünden unter Anwendung IT-forensischer Prinzipien gesichert und dadurch für eine Vielzahl von Anwendungsmöglichkeiten nutzbar gemacht werden können. Hierzu wurden fünf exemplarische Rollen vorgestellt und ihre individuellen Anforderungen an die zu sichernden Daten diskutiert. Ein Konzept auf Basis eines hybriden kryptographischen Verfahrens wurde vorgestellt und zusammen mit der rollenindividuellen Datenfilterung anhand einer prototypischen Umsetzung illustriert. Abschließend wurden ausgewählte Vor- und Nachteile des Konzeptes diskutiert.

Auch weitere offene Punkte sollten in zukünftigen Arbeiten noch vertieft adressiert werden. Hinsichtlich des Prototyps ist der Ressourcenbedarf des FFDS (Rechenzeit, Speicherplatz) anhand anwendungsnaher Filterregeln und CAN-Kommunikation zu untersuchen. Insbesondere aufgrund des hohen Kostendrucks in der Automobilindustrie ist dies essentiell für die Rechtfertigung eines praktischen Einsatzes. Des Weiteren ist bezüglich des Konzeptes noch der Fall vertieft zu berücksichtigen, dass der Fahrzeugbesitzer (R1) zumindest zeitweilig nicht mit dem Fahrzeugführer übereinstimmen muss. Hinsichtlich von Datenschutzaspekten müsste hier noch feingranularer zwischen verschiedenen Fahrzeugführern unterschieden werden, was sich beispielsweise mit biometrischen Systemen zu Insassenauthentikation [BS07] kombinieren ließe. Auch adressiert das Konzept aktuell nur digitale Daten von den Fahrzeugbussen. Darüber hinaus kann es sinnvoll sein, weitere Informationen (ausgewählte Sensorwerte, interne Betriebsdaten von Steuergeräten, …) mit einzubeziehen. Trotz der in Abschnitt 5 skizzierten Angriffsszenarien sollten in den Prozessen (z.B. Wartung) auch zulässige Möglichkeiten vorgesehen werden, einen Wechsel des FFDS (z.B. bei Defekt) oder des Fahrzeugs (z.B. bei Neukauf) vornehmen zu können.

Danksagungen: In Teilen wurde diese Veröffentlichung durch die Europäische Union im Kontext des Verbundprojekts COmpetence in MObility (C-2007-5254) unterstützt. Teile der Erkenntnisse zu den Grundlagen der IT-Forensik dieser Arbeit entstanden aus der Bearbeitung eines Projektes des Bundesamts für Sicherheit in der Informationstechnologie (BSI). The work described in

this paper has been supported in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II.

Literaturverzeichnis

[HKD08] Hoppe, T.; Kiltz, S.; Dittmann, J.: Security threats to automotive CAN networks – practical examples and selected short-term countermeasures. In: SAFECOMP 2008, Springer LNCS 5219, ISBN 978-3-540-87697-7, 2008; S. 235-248.

[Ko10] Koscher, K. et.al.: Experimental Security Analysis of a Modern Automobile. In: The IEEE Symposium on Security and Privacy, Oakland, CA, May 16-19, 2010.

[BM09] Burg, H.; Moser, A. (Hrsg.): Handbuch Verkehrsunfallrekonstruktion, 2., aktualisierte Auflage, Verlag Vieweg + Teubner, ISBN 978-3-8348-0546-1, 2009.

[Bo08] Borgeest, K.: Elektronik in der Fahrzeugtechnik - Hardware, Software, Systeme und Projektmanagement, 1. Auflage 2008, Vieweg Verlag, ISBN 978-3-8348-0207-1, 2008.

[BD07] Barisani, A.; Bianco, D.: Unusual Car Navigation Tricks: Injecting RDS-TMC Traffic Information Signals. In: Can Sec West, Vancouver, 2007.

[MFA10] MyFox Austin: Hacker Deactivates 100 Cars Via Internet, 17.3.2010, http://www.myfoxaustin.com/dpp/news/local/31710-Hacker-Deactivates-100-Cars-Via-Internet, Letzter Zugriff: 16.6.2010.

[HKD09] Hoppe, T.; Kiltz, S.; Dittmann, J.: Applying Intrusion Detection to Automotive IT – Early Insights and Remaining Challenges. In: Journal of Information Assurance and Security (JIAS), ISSN: 1554-1010, Vol. 4, Issue 6, 2009; S. 226-235.

[MHD10] Müter, M.; Hoppe, T.; Dittmann, J.: Decision Model for Automotive Intrusion Detection Systems. Erscheint in: Automotive - Safety & Security 2010, Ada Deutschland Tagung 21. - 23. Juni 2010, Stuttgart, Shaker Verlag, Aachen, 2010.

[KHA09] Kiltz, S.; Hildebrandt, M.; Altschaffel, R.; Dittmann, J.; Vielhauer, C.; Schulz, C.: Sicherstellung von gelöschtem Schadcode anhand von RAM- Analysen und Filecarving mit Hilfe eines forensischen Datenmodells. In: 11. Deutscher IT-Sicherheitskongress, Bonn 2009, SecuMedia Verlag Ingelheim, ISBN 978-3-922746-97-3, 2009; S. 473-488.

[Ho10] Holthusen, S.: Datenerhebung aus Fahrzeugnetzwerken nach IT-forensischen Prinzipien, Bachelorarbeit, Universität Magdeburg, 2010.

[Ha03] Harms, D.: Unfalldatenspeicher (UDS) als möglicher Beitrag zur Verkehrssicherheit im Meinungsbild Jugendlicher und Heranwachsender, Dissertation, Braunschweig, 2003.

[EDR06] National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT): Event Data Recorders - Final Rule, Docket No. NHTSA-2006-25666, 2006.

[ZS08] Zimmermann, W.; Schmidgall, R.: Bussysteme in der Fahrzeugtechnik - Protokolle und Standards, 3., Auflage, Vieweg Verlag, ISBN 978-3834804471, 2008.

[MR10] MyRate Program, http://www.progressive.com/myrate/, Letzter Zugriff: 16.6.2010.

[KH02] Kruse, W.; Heiser, J.: Computer Forensics – Incident Response Essentials, Addison Wesley, ISBN 0201707195, 2002.

[Bu10] Buchmann, J.: Einführung in die Kryptographie, 5. Auflage, Springer-Verlag, ISBN 978-3-642-11185-3, 2010.

[Eck03] Eckert, C.: IT-Sicherheit, Oldenbourg, ISBN 3-486-27205-4, 2003.

[BZ08] Detlef Borchers, Peter-Michael Ziegler: Mit PKI gegen den Autoklau, Heise Newsticker 5.3.2008, http://www.heise.de/newsticker/meldung/104593, 2008.

[We09] Weyl, B. et. al.: Securing Vehicular On-Board IT Systems: The EVITA Project. In: 25. VDI/VW Gemeinschaftstagung - Automotive Security (CD-Rom), Düsseldorf, VDI Wissensforum GmbH, 2009.

[BS07] Büker, U.; Schmidt, R.: Biometrische Fahreridentifikation. In: 23. VDI/VW Gemeinschaftstagung - Automotive Security, VDI-Berichte Nr. 2016, VDI-Verlag, 2007.