Sicherheit in automobilen Bussystemen

Marko Wolf [1], André Weimerskirch [1,2], Christof Paar [1,2]

[1] Horst Görtz Institut (HGI) für Sicherheit in der Informationstechnik,
Ruhr-Universität Bochum

[2] escrypt GmbH, Bochum

{mwolf,weika,cpaar}@crypto.rub.de

Zusammenfassung: In dieser Arbeit werden aktuelle und zukünftige Automobilbussysteme auf ihre Sicherheit gegenüber gezielt manipulierenden Angriffen analysiert. Nach einer kurzen technischen Beschreibung verschiedener repräsentativer Automobilbussysteme werden mögliche Angreifer, denkbare Angriffsszenarios und Gefahrenpotenziale im Automobilbereich erläutert. Die abschließende Beispielimplementierung nutzt moderne kryptographische Mechanismen zur Geheimhaltung, Manipulationssicherheit und Authentisierung, welche in der Lage sind, die wesentlichsten Herausforderungen zur Kommunikationssicherheit im Automobilbereich zu lösen.

Schlüsselwörter: Automobile Kommunikationssicherheit,
Fahrzeugbussysteme, Angriffe, Authentifizierung, Verschlüsselung,
Firewalls, LIN, CAN, FlexRay, MOST, Bluetooth

1 Einführung

Die fortschreitende „Elektronisierung“ des Automobils (Tabelle 1) erreicht immer größere Ausmaße. Moderne Kraftfahrzeuge enthalten heute schon eine Vielzahl von Steuergeräten, welche über verschiedenste Kommunikationsnetzwerke miteinander verbunden sind. Automobile Datenübertragungssysteme haben Zugang zu einer Vielzahl sicherheitskritischer Fahrzeugsysteme, wie Bremsen, Airbag oder Motorsteuerung. Fahrzeuge, welche heute schon über Fahrdynamikprogramme wie ESP (*Electronic Stability Program*) oder ACC (*Adaptive Cruise Control*) verfügen, erlauben besonders weit reichende Eingriffe ins Fahrverhalten.

Zukünftige, vollkommen elektronische *Drive-by-Wire* Fahrzeugsysteme nutzen für sämtliche Steuerkommandos die entsprechenden Automobilnetzwerke. Während die Funktionssicherheit (*safety*) automobiler Kommunikationssysteme gegenüber zahlreichen technischen Störungen weitestgehend gewährleistet wird, wurden zur Abwehr böswilliger, gezielt manipulierender Angriffe (*security*) bisher kaum Maßnahmen ergriffen. Die zunehmende Vernetzung der gegenüber gezielten Angriffen noch ungesicherten Fahrzeugbusse mit den neuen Fahrzeugmultimedianetzwerken wie GigaStar oder MOST (*Media Oriented System Transport*) und vor allem die Einführung drahtloser Kommunikationsschnittstellen wie GSM (*Global System for Mobile Communications*) oder Bluetooth erfordern weitergehende Überlegungen zur automobilen Kommunikationssicherheit.

Elektronische Einspritzung Zentrale Hinweisleuchten Zentralverriegelung Tempomat	Automatikschaltung Antiblockiersystem Klimaautomatik Autotelefon Elektronische Spiegel	Airbag Navigationssystem Fahrerassistenzsysteme Elektr. Verkehrsführung Sprachsteuerung	Drive-by-Wire Internet Telematik Ad-hoc Netzwerke Personalisierung
1970er	1980er	1990er	2000er

Tabelle 1: *Elektronikentwicklung im Automobil nach [We02]*

Abschnitt 2 gibt einen kurzen Überblick der bekanntesten, aktuellen und zukünftigen Fahrzeugkommunikationssysteme. Abschnitt 2.1 nennt die wichtigsten technischen Merkmale und Übertragungseigenschaften von jeweils einem typischen Vertreter aus jeder Fahrzeugbusklasse. In Abschnitt 2.2 werden zwei Methoden zur Verkopplung verschiedener Bussysteme kurz erläutert. Abschnitt 3 behandelt die Gefährdung automobiler Bussysteme. Es werden mögliche Angreifer und Angriffsziele sowie eine Reihe von Angriffstechniken für den jeweiligen repräsentativen Vertreter jeder Busklasse vorgestellt. Abschnitt 4 erläutert einfache kryptographische Methoden, welche die automobile Kommunikationssicherheit erheblich verbessern können, sowie den Entwurf einer Beispielimplementierung.

2 Fahrzeugkommunikationssysteme

Die Anzahl der im Automobilbereich verwendeten Kommunikationssysteme ist besonders vielfältig. Die möglichen Einsatzgebiete reichen von der Motorsteuerung über diverse Fahrdynamikprogramme und Sicherheitsmechanismen bis hin zu unzähligen Komfort- und Infotainmentanwendungen. Wie in Tabelle 2 dargestellt, lassen sich automobile Bussysteme nach ihren grundlegenden Eigenschaften und Einsatzgebieten in fünf verschiedene Klassen einteilen.

Klasse	Subbus	Ereignisgesteuert	Zeitgesteuert	Multimedia	Drahtlos
Vertreter	LIN K-Line I^2C	CAN VAN PLC	FlexRay TTP TTCAN	MOST D2B GigaStar	Bluetooth GSM WLAN
Maximale Datenrate [MBit/s]	≤ 0.02	≤ 1	1 - 10	10 - 25	≤ 1
Relative Kosten pro Netzknoten	0.5	1	2.5	5	5

Tabelle 2: *Klassifizierung von Automobilbussystemen*

Kleine lokale Subbusse wie LIN (*Local Interconnect Network*) steuern beispielsweise die automatische Türverriegelung, elektrische Fensterheber und Spiegel. Zudem werden sie zur Kommunikationen mit diversen intelligenten Sensoren eingesetzt, welche unter anderem Dunkelheit oder einsetzenden Regen feststellen können. Die Klasse der ereignisgesteuerten Busse, wie CAN (*Controller Area Network*) oder VAN (*Vehicle Area Network*) ermöglicht die fast echtzeitfähige Kommunikation für Anwendungen wie ABS (*Antilock Breaking System*) oder die Motorsteuerung. Zeitgesteuerte und hart echtzeitfähige Bussysteme wie FlexRay, TTCAN (*Time-Triggered* CAN) oder TTP (*Time-Triggered Protocol*) garantieren deterministische Übertragungszeiten zwischen den einzelnen Steuergeräten und bieten damit die technische Basis für zukünftige hochsicherheitskritische *Drive-by-Wire* Fahrzeugssysteme. Die meist auf Glasfaserverbindungen basierenden Multimediabussysteme wie MOST, D2B (*Domestic Digital Bus*) oder GigaStar entwickelten sich aus den stetig wachsenden Anforderungen der verschiedensten automobilen Unterhaltungsanwendungen (*In-Car Entertainment*) nach besonders breitbandigen Hochleistungskommunikationssystemen zur Übertragung qualitativ hochwertiger Video-, Audio- und Sprachdaten innerhalb des Fahrzeugs. Die Klasse der drahtlosen Kommunikationssysteme enthält verschiedene drahtlose Übertragungstechnologien, welche mehr und mehr auch im automobiler Bereich Einzug halten. Sie ermöglichen die Kommunikation des internen Fahrzeugnetzes

mit umgebenden Fahrzeugen sowie die Nutzung zahlreicher drahtloser Informationssysteme (*Location Based Services*).

2.1 Verschiedene repräsentative Bussysteme

Anschließend erfolgt eine kurze Beschreibungen der wesentlichsten technischen Merkmale und Übertragungseigenschaften jeweils eines repräsentativen Vertreters aus jeder Busklasse. Weiterführende Informationen sind in [Do02, He02, Kr02, Ra02, RT03] zu finden.

CAN: Das am weitesten verbreitete, ereignisgesteuerte CAN (*Controller Area Network*) Bussystem wurde 1981 von der Firma Bosch entwickelt (seit 1994 als ISO 11898 auch international genormt) und dient dem schnellen, seriellen Datenaustausch (bis 1 MBit/s) zwischen den elektronischen Steuergeräten eines Fahrzeugs. Alle Steuergeräte eines CAN-Netzwerkes sind gleichberechtigt und besitzen Masterfunktionalität (*multi master architecture*), das heißt jedes Steuergerät kann Nachrichten versenden, und der Ausfall eines Steuergerätes führt nicht zum Ausfall des gesamten Bussystems. CAN-Nachrichten enthalten keinen direkten Empfänger, sondern werden mittels einer 11 Bit (CAN20A) bzw. 29 Bit (CAN20B) langen Nachrichtenkennung (*identifier*) eindeutig typisiert. Jeder CAN-Busteilnehmer empfängt stets alle Nachrichten und entscheidet selbst, mit Hilfe geeigneter Akzeptanzfilter, welche Nachrichten zur Weiterverarbeitung übernommen werden. Dieses *Broadcasting* ermöglicht, dass eine gesendete Nachricht von einem, mehreren oder allen Steuergeräten gleichzeitig empfangen und verarbeitet werden kann. Zur Zugriffssteuerung wird in einem CAN-Netzwerk das dezentrale, prioritätengesteuerte und verlässliche (*reliable*) CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*) Verfahren eingesetzt. Dabei wird anhand der, der Nachrichtenkennung zugeordneten Priorität entschieden, welches sendebereite Steuergerät seine Nachricht übermitteln darf. Diese Methode garantiert zu jedem Zeitpunkt die Übertragung der höchstprioren CAN-Nachricht mit Latenzzeiten im μs-Bereich. Um den Einsatz von CAN auch in der Umgebung starker elektromagnetischer Felder zu ermöglichen, wird eine Fehlerbehandlung eingesetzt, welche Übertragungsfehler erkennt, die fehlerhafte Übertragung mit der Aussendung eines Fehlerflags (*error flag*) abbricht, eine erneute Übertragung der betroffenen CAN-Nachricht einleitet und gleichzeitig die Übernahme der CAN-Botschaft durch andere Steuergeräte verhindert. Desweiteren enthält das CAN-Protokoll Mechanismen zur automatischen Fehlereingrenzung, bis hin zur Abschaltung der defekten Steuergeräte.

LIN: LIN (*Local Interconnect Network*) ist ein auf den UART (*Universal Asynchronous Receiver Transmitter*) Standard basierendes Eindraht (*single wire*) Netzwerk zur kostengünstigen, seriellen Kommunikation zwischen intelligenten Sensoren und Aktoren mit Übertragungsraten von bis zu 20 kBit/s. Der vom LIN-Konsortium (u.a. Audi, BMW, DaimlerChrysler, Volkswagen, Volvo) konzipierte, offene Standard wird ab 2001 überall dort eingesetzt, wo die Leistungsfähigkeit eines CAN-Netzwerkes nicht benötigt wird. Ein LIN-Bussystem besteht aus einem *Master* und bis zu 16 *Slaves*. Der LIN-Master steuert allein die kollisionsfreie Datenübertragung, optional für quarzlose Steuergeräte auch inklusive einer Zeitsynchronisation. LIN ist analog zu CAN ein empfängerselektives Bussystem. Fehlerhaft übertragene LIN-Nachrichten werden mittels Paritätsbits und einer Prüfsumme erkannt und verworfen. Die LIN-Spezifikation sieht zudem zwei Netzknotenzustände vor: *Sleep-Mode* und *Normal-Mode*. Der Übergang zwischen den beiden Modi wird einerseits mit einem expliziten Kommando vom LIN-Master oder über ein *Wake-Up-Signal-Frame* von einem LIN-Slave initiiert. LIN-Subnetze werden zur Ansteuerung über einen geeigneten Netzübergang (*Gateway*) an das übergeordnete CAN-Netzwerk angeschlossen.

FlexRay: FlexRay ist ein auf den Entwicklungen von DaimlerChrysler und BMW (*ByteFlight*) basierender, flexibler, deterministischer und fehlertoleranter Hochgeschwindigkeitsbus, welcher

mit Übertragungsgeschwindigkeiten von bis zu 10 MBit/s (*single channel*, redundant) bzw. 20 MBit/s (*dual channel*) den Anforderungen zukünftiger Automobilanwendungen entspricht. Das FlexRay-Konsortium (u.a. BMW, DaimlerChrysler, Motorola, Philips, GM, Bosch) plant den Einsatz von FlexRay in der Fahrzeug-Serienproduktion ab etwa 2006. Das flexibel erweiterbare FlexRay-Netzwerk besteht aus bis zu 64, mit aktiven Sternkopplern Punkt-zu-Punkt verbundenen, Netzknoten und kann mit Einschränkungen auch in klassischer Busstruktur betrieben werden. Als Übertragungsmedium (*Physical Layer*) eignen sich sowohl Lichtleiter als auch Kupferleitungen. Die Kanalredundanz im *single-channel* Modus ermöglicht, dass die Übertragung auch bei Leitungsunterbrechungen oder ausgefallenen Netzknoten aufrechterhalten werden kann. Die Adressierung von FlexRay-Botschaften erfolgt, analog zu CAN, empfängerselektiv. Logische Fehler, wie eine Busmonopolisierung durch ein fehlerhaftes Steuergerät (*Babbling Idiot*), werden von einer unabhängige Instanz (*Bus Guardian*) erkannt und z.B. durch Abtrennung des entsprechenden Steuergerätes behoben. Zusätzlich wird der gesamte Kommunikationsweg (*end-to-end*) durch die deterministische Datenübertragung und durch ein Protokoll-CRC abgesichert. Das verwendete zyklische TDMA-Übertragungsschema (*Time Division Multiple Access*) ermöglicht über frei konfigurierbare, statische und dynamische Zeitsegmente, sowohl die asynchrone Übertragung zeitunkritischer Daten, als auch die synchrone Übertragung zeitkritischer Informationen. Die jedem Netzknoten zugeordneten Zeitfenster (*time slots*) des statischen Segments garantieren die deterministische Datenübertragung. Im gemeinsam genutzten, dynamischen Segment erfolgt die Zuteilung der Bandbreite prioritätsgesteuert. Die dafür notwendige, gemeinsame Zeitbasis (*global time*) wird mittels Synchronisationsnachrichten im statischen Teil des Zyklus realisiert.

MOST: Der vorrangig für Multimedia- und Telematikanwendungen konzipierte, serielle MOST (*Media Oriented Systems Transport*) Hochgeschwindigkeitsbus wird seit 1998 von der MOST Cooperation (u.a. BMW, DaimlerChrysler) entwickelt und bereits seit 2002 in Serienfahrzeugen eingesetzt. Das auf einem optischen Übertragungsmedium basierende *Peer-to-Peer* Netzwerk ermöglicht, via *Plug'n Play*, bis zu 64 MOST-Geräten die synchrone (bis 24 MBit/s) und asynchrone (bis 14 MBit/s) Datenübertragung in Ring-, Stern- oder Busanordnung. Ein MOST-Frame enthält, analog zu FlexRay, zwei variable Bereiche für die synchrone und asynchrone Datenübertragung, sowie einen festen Bereich für den Kontrollkanal. Über den Kontrollkanal können MOST-Geräte, ähnlich wie einem Telefonnetz, Datenkanäle anfordern oder wieder freigeben. Die zu übertragenen MOST-Nachrichten enthalten, im Gegensatz zum empfängerselektiven CAN, stets eine eindeutige Absender- und Empfängerkennung. Die MOST-Zugriffssteuerung erfolgt bei der synchronen Übertragung mittels TDM (*Time Division Multiplex*) und bei der asynchronen Übertragung mittels CSMA/CA. Die Synchronisation des Netzwerkes steuert ein MOST-Gerät (*Timing Master*) mittels kontinuierlich, an alle angeschlossenen *Timing Slaves* versendete Synchronisations-Frames. Das Fehlermanagement erledigt ein interner MOST-Systemservice, welcher Fehler mit Hilfe von Paritätsbits, Statusflags und CRC-Prüfsummen erkennt und ggf. fehlerhafte MOST-Geräte von der Kommunikation ausschließt. MOST ist ISO/OSI standardisiert, unterstützt Netzwerkprotokolle wie TCP, diverse Streaming Formate (z.B. MPEG) und bietet zudem Schnittstellen zu GSM, GPS oder Bluetooth.

Bluetooth: Ursprünglich entwickelt um unterschiedliche Systeme wie Computer und Mobiltelefone miteinander zu verbinden, ist Bluetooth heute einer der wichtigsten drahtlosen Funkübertragungsstandards. Im lizenzfreien 2.45 GHz ISM-Band (*Industrial, Scientific and Medical*) ermöglich Bluetooth die drahtlose Ad-hoc Vernetzung verschiedenster Geräte wie PDAs (*Personal Digital Assistent*), Mobiltelefone, Laptops, Drucker oder Digitalkameras, um Daten über kurze Distanzen von bis zu 100 Metern auszutauschen. Konzipiert als preiswertes Transceivermodul mit möglichst geringem Energieverbrauch, sind Datenraten von bis zu 700 kBit/s möglich. Innerhalb der nur bedingt *Multi-Master* fähigen, so genannten *Piconets*, unterstützt ein einzelnes Bluetooth-Gerät bis zu sieben Punkt-Zu-Punkt oder Punkt-Zu-Mehrpunkt Ver-

bindungen, welche optional auch verschlüsselt sein können.

Die nachfolgende Tabelle 3 gibt einen zusammenfassenden Überblick der wesentlichen Kenndaten vorgenannter Bussysteme.

Bus	**LIN**	**CAN**	**FlexRay**	**MOST**	**Bluetooth**
Geeignet für	Untergeordnete Subnetze	Weiche Echtzeitsysteme	Harte Echtzeitsysteme	Multimedia Telematik	Externe Kommunikation
Mögliche Zielanwendungen	Zentralverriegelung Klimasteuerung Fensterheber Licht-, Regensensor	Antiblockiersystem Fahrassistenten Motorsteuerung Automatikschaltung	Break-by-Wire Steer-by-Wire Shift-by-Wire Notfallsysteme	Unterhaltung Navigation Informationsdienste Mobiles Büro	Telematik Mauterfassung Internet Telefon/Notruf
Architektur	Single-Master	Multi-Master	Multi-Master	Multi-Master	Multi-Master
Zugriffsverfahren	Polling	CSMA/CA	TDMA FTDMA	TDM CSMA/CA	TDMA TDD
Übertragungs-Modus	Synchron	Asynchron	Synchron Asynchron	Synchron Asynchron	Synchron Asynchron
Datenrate	20 kBit/s	1 MBit/s	10 MBit/s	24 MBit/s	720 kBit/s
Redundanz	Keine	Keine	2 Kanäle	Keine	79 Frequenzen
Fehlererkennung	Checksumme Paritätsbits	CRC Paritätsbits	CRC Bus Guardian	CRC Systemservice	CRC FEC
Physikalische Schicht	Eindrahtleitung	Zweidrahtleitung	Lichtleitfaser Zweidrahtleitung	Lichtleitfaser	Luft

Tabelle 3: *Eigenschaften ausgewählter Automobilbussysteme*

2.2 Netzübergänge

Damit Bussysteme trotz ihrer unterschiedlichen Protokolle, Übertragungsmethoden und physikalischen Schnittstellen miteinander kommunizieren können, sind geeignete Netzübergänge (*Bridges* oder *Gateways*) notwendig. Diese Netzübergangsmodule lesen und schreiben von und zu allen verfügbaren Busschnittellen, realisieren die Protokollumsetzung sowie die Fehlererkennung. Abhängig von ihrer jeweiligen Verkopplung können bestimmte Schnittstellen eines *Gateways* auf das Senden oder auf das Empfangen von Daten beschränkt sein. Zudem ist die Implementierung einfacher Filterregeln auf der Ebene der jeweils angeschlossenen Bussysteme möglich. Während entweder so genannte *Supergateways* zentral alle im Fahrzeug verwendeten Bussysteme miteinander verbinden, verkoppeln *Bridges* jeweils nur zwei verschiedene Bussysteme miteinander. *Supergateways* benötigen daher meist eine relativ komplexe Software sowie genügend Rechenleistung, um alle notwendigen Protokollumsetzungen in ausreichender Geschwindigkeit realisieren zu können, wohingegen *Bridges* die Hard- und Softwareumsetzung nur zwischen zwei verschiedenen Bussystemen beherrschen müssen. Die zusätzlichen Kosten und die erhöhte Anfälligkeit einer busübergreifenden Kommunikation mittels einer Vielzahl von *Bridges*, lässt jedoch Automobilhersteller gegenwärtig eher zum Einsatz von *Supergateways* tendieren. Aktuelle *Supergateways* (z.B. Motorola TCU) bieten überdies, neben der Umsetzung fast aller gängigen Fahrzeugkommunikationssysteme, auch schon eine Vielzahl von drahtlosen Telekommunikationsschnittstellen wie GSM, UMTS, Bluetooth oder WLAN.

3 Gefahrenpotenziale

Elektronische Fahrzeugbauteile sind seit jeher lohnende Ziele für gezielte Eingriffe oder Manipulationen. Tachometerrückstellung [Mos04], unautorisiertes Chiptuning oder Fahrtenschreibermanipulation [An98] sind schon heute, häufig praktizierte, aber noch relativ harmlose Beispiele

für Erfolg versprechende Eingriffe in die Fahrzeugelektronik. Zukünftige elektronische Automobilanwendungen wie der digitale Fahrtenschreiber, die elektronische Maut, das elektronische Nummerschild oder die Vielzahl neuer kostenpflichtiger Informationsdienste (*Location Based Services*) werden den Anreiz zur Manipulation elektronischer Bauteile weiter erhöhen. Allein der Versuch einer unautorisierten Modifikation kann die Fahrsicherheit des betroffenen Fahrzeugs und umgebender Verkehrsteilnehmer gefährden.

Neben dem augenscheinlichsten Angreifer, dem Fahrzeugbesitzer, sind entsprechend angewiesenes Werkstattpersonal oder Dritte, wie beispielsweise konkurrierende Hersteller oder andere unautorisierte Personen oder Institutionen, mögliche Angreifer auf die Fahrzeugelektronik. Vergleicht man die Fähigkeiten und Zugriffsmöglichkeiten von Angreifern im Automobilbereich, mit denen in herkömmlichen Computernetzwerken, ergeben sich deutliche Unterschiede. Während Angreifer in einem Computernetzwerk eher selten physikalischen Zugriff zum attackierten System haben werden, verfügen das Personal einer Autowerkstatt und der Fahrzeugbesitzer über den uneingeschränkten, physikalischen Zugriff auf die Fahrzeugelektronik. Während der Fahrzeugbesitzer in der Regel nur über ein geringes technisches Verständnis und nur über wenige geeignete Gerätschaften verfügt, haben Autowerkstätten mit der Kombination aus physikalischem Zugriff und ausreichend hohem, technischen Verständnis sowie entsprechend geeigneten Hilfsmitteln besonders gute Möglichkeiten, tief greifende und dauerhafte Veränderungen an der Automobilelektronik vorzunehmen. Denkbare Angriffe Dritter ohne direkten physikalischen Zugang zum Fahrzeug, sind beispielsweise Angriffe auf die Privatsphäre (Telefonüberwachung, Datendiebstahl) oder die gezielte Störung einzelner Fahrzeugkomponenten (Diebstahl, Anschlag). In Tabelle 4 sind die drei potenziellen Angreifergruppen und ihre jeweiligen Befähigungen kurz dargestellt. Offensichtlich ist das technisch versierte, im Auftrag des Fahrzeugbesitzers handelnde, Werkstattpersonal die gefährlichste Angreifergruppe.

Angreifer	**Fähigkeiten**	**Physikalischer Zugang**
Fahrzeugbesitzer	Variiert (i.A. Niedrig)	Vorhanden
Werkstattpersonal	Hoch	Vorhanden
Dritte	Variiert (ggf. Hoch)	Keinen

Tabelle 4: *Angreifer im Automobilbereich nach [Pa03]*

Während bisherige Sicherheitsanalysen [Pl02, Po01] vor allem die Zuverlässigkeit und die korrekte Handhabung zufällig auftretender Fehler in Fahrzeugnetzwerken untersucht haben, sind moderne Automobilkommunikationssysteme gezielt manipulierenden Angriffen weitestgehend ungeschützt ausgeliefert. Die Ursachen hierfür sind vielfältig. Da bisher vor allem der Zuverlässigkeit (*safety*) im Vordergrund stand, war die Implementierung von Kommunikationssicherheit (*security*), wenn überhaupt, meist nur ein nachträglicher und halbherziger Prozess. Die besonderen technischen und finanziellen Beschränkungen, die Vielzahl der involvierten Parteien (Zulieferer, Hersteller, Werkstatt, Besitzer, etc.) und das oft unzureichende kryptographische Know-how verursachen zusätzlich Schwierigkeiten bei der Umsetzung zweckmäßiger Schutzmassnahmen. Zudem erzeugen die zusätzliche Hard- und Software sowie die notwendige kryptographische Infrastruktur zusätzliche Kosten, ohne einen offensichtlich erkennbaren Mehrwert. Die trotz der mangelnden Kommunikationssicherheit, stetig fortschreitende Elektronikentwicklung und die damit verbundene, zunehmende Vernetzung, wird mehr und mehr zu einem ernsten Problem, dessen Lösung - die Bereitstellung leistungsfähiger, kostengünstiger automobiler Kommunikationssicherheit - eine der zukünftigen Herausforderungen im Bereich der Automobilelektronik darstellen wird.

Der unkontrollierte Eingriff in die Bussysteme eines Fahrzeugs wird durch viele Faktoren relativ leicht ermöglicht. Beispielsweise erfolgt jegliche Kommunikation innerhalb und zwischen einzelnen Bussystemen vollkommen unverschlüsselt im Klartext. Mögliche Botschaften und

deren Aufbau sind für fast alle Fahrzeugnetze öffentlich verfügbar. Zudem erfolgt keinerlei Authentisierung, ob eine empfangene Nachricht überhaupt von einem zulässigen Steuergerät versendet wurde.

Das größte Gefahrenpotenzial ergibt sich jedoch aus der weitgehend ungesicherten Kommunikation der verschiedenen Fahrzeugbussysteme miteinander. Der über *Gateways* gesteuerte, netzübergreifende Datenaustausch ermöglicht potenziell den Zugriff aus jedem beliebigen Netz heraus, hinein in ein beliebiges anderes Fahrzeugnetz. Das heißt, ein jedes LIN-, CAN- oder MOST-Steuergerät ist potenziell in der Lage, Nachrichten in alle anderen vorhandenen Busnetze zu versenden. Folglich reicht schon einzelnes kompromittiertes Bussystem, um das gesamte automobile Kommunikationsnetzwerk zu gefährden. Mit der Integration zahlreicher drahtloser Kommunikationsschnittenstellen können Angriffe sogar berührungslos *im Vorbeifahren* oder gar per GSM, tausendfach, von nahezu jedem Ort der Welt erfolgen. Zukünftige Bildverarbeitende Systeme zur autonomen Fahrzeugsteuerung haben Zugang zu allen elementaren Fahrzeugsystemen, basierend auf Informationen, welche sie von externen Datenbanken über nur unzulänglich gesicherte, drahtlose Verbindungen erhalten haben. Zudem erlaubt die Verkopplung der verschiedenen Multimedianetzwerke mit den Steuerungsnetzwerken des Fahrzeugs, Angriffe durch Softwareprogramme wie Viren oder Würmer, welche sich über eingelegte CD/DVDs, empfangene Email-Nachrichten oder eventuell angeschlossene Notebooks oder PDAs Zugang zu allen sicherheitsrelevanten Fahrzeugsystemen verschaffen können. Selbst wenn moderne *Gateways* schon einfache Zugangsschutzsysteme (*Firewalls*) integrieren, verfügen fast alle über völlig ungesicherte Diagnoseschnittstellen und -funktionen, welche den uneingeschränkten Zugang zum gesamten Fahrzeugnetzwerk ermöglichen.

Die Konsequenzen eines erfolgreichen Angriffs reichen von einfachen Einschränkungen des Komforts bis zur Gefahr eines Unfalls. Folglich werden die notwendigen Sicherheitsmaßnahmen für das jeweilige Bussystem durch die möglichen Folgen eines erfolgreichen Angriffs bestimmt. Während, wie in Tabelle 5 aufgeführt, Angriffe auf LIN- oder Multimedianetzwerke etwa nur zur Störung der elektrischen Fensterheber oder des Navigationssystems führen können, gefährden Eingriffe in den CAN-Bus durch mögliche Fehlfunktionen wichtiger Fahrerassistenzsysteme ernsthaft die Fahrsicherheit. Unkontrollierte Eingriffe in Echtzeitbusse wie FlexRay, welche direkt Steuerkommandos zu den Bremsen oder zur Lenkung übertragen, bedeuten eine akute Gefahr für die betroffenen Passagiere und allen anderen umgebenden Verkehrsteilnehmer. Nichtsdestotrotz kann schon der einfache Ausfall der Türentriegelung gravierende Folgen für die betroffenen Insassen nach sich ziehen [BaP03].

Klasse	Subbus	Ereignisgesteuert	Zeitgesteuert	Multimedia	Drahtlos
Vertreter	LIN	CAN	FlexRay	MOST	Bluetooth
Gefährdung	Klein	Groß	Akut	Klein	Variiert
Mögliche Folgen	Eingeschränkte Funktionalität	Eingeschränkte Fahrsicherheit	Unfall-gefahr	Datenverlust, Komfortminderung	Unautorisierter Datenzugriff

Tabelle 5: *Gefährdungspotenziale ausgewählter Automobilbussysteme*

Mit der Möglichkeit beliebige Nachrichten in alle Bussystemen zu versenden, sind gezielte Angriffe auf jeweils spezielle Applikationen (Steuerungssoftware, Fahrtenschreiber, etc.) oder generelle Angriffe zum Ausfall einzelner Steuergeräte oder eines gesamten Bussystems möglich. Nachfolgend werden einige mögliche Attacken auf die jeweils repräsentativen Bussysteme aus Abschnitt 2.1 kurz beschrieben. Alle Angriffe benötigen nur den logischen Netzzugang, welcher auch über die Vielzahl der drahtlosen Schnittstellen erlangt werden kann.

LIN: Gezielt versendete *Sleep-Frames* können einzelne Steuergeräte so lange deaktivieren, bis ein *Wake-Up-Frame* des übergeordneten CAN-Busses den korrekten Zustand wiederherstellt.

Attacken auf die LIN-Synchronisation mittels manipulierter *SYNCH* Nachrichten oder die gezielte Deaktivierung des jeweiligen LIN-Masters schalteten den betroffenen LIN-Bus vollständig ab.

CAN: Der prioritätsgesteuerte CSMA/CD Zugangskontrollmechanismus von CAN erlaubt so genannte *Jamming Attacks*, welche durch permanente höchstpriore Nonsensnachrichten den Kommunikationskanal für alle anderen Steuergeräte blockieren. Zudem kann der Mechanismus zur automatischen Fehlereingrenzung ausgenutzt werden, um über systematisch versandte Fehlerflags, gezielt einzelne Steuergeräte vom CAN-Netz zu trennen.

FlexRay: Analog zur automatischen Fehlereingrenzung von CAN, kann der *Bus Guardian* von FlexRay missbraucht werden, um mit Hilfe gefälschter Fehlermeldungen gezielt einzelne Steuergeräte abzuschalten. Angriffe auf die gemeinsame Zeitbasis aller Netzknoten sind ebenfalls möglich, wenn innerhalb eines statischen Kommunikationszyklus mehr als f [1] manipulierte Synchronisationsnachrichten eingeschleust werden. Zusätzlich können FlexRay Steuergeräte, welche über einen Energiesparmodus verfügen, mittels geeigneter *Sleep-Frames* gezielt deaktiviert werden.

MOST: Auch in MOST Bussen können eingeschleuste manipulierte Synchronisationsnachrichten den Synchronisierungsmechanismus erheblich stören oder völlig abschalten. Systematische, ungenutzte *Channel Requests* reduzieren die verbleibende Bandbreite für alle übrigen MOST-Knoten auf ein Minimum beziehungsweise können die Kommunikation ganz unterbinden. Angriffe mittels verfälschter *Boundary Descriptors* oder *Jamming Attacks* auf den prioritätsgesteuerten Asynchron- oder Kontrollkanal sind ebenfall möglich.

Bluetooth: Obwohl Bluetooth auch verschlüsselte Verbindungen ermöglicht, existieren einige praktikable Angriffe [Ast03, BSI03, JS01]. Es existieren sogar schon erste Würmer und Viren, welche Bluetoothgeräte drahtlos infizieren können [Cab04, Spg04].

4 Lösungsansätze

Die Mehrzahl der zukünftigen Fahrzeuganwendungen setzt für ihre Realisierung ein Höchstmaß an Kommunikationssicherheit voraus. Dazu gehören unter anderem, dass kritische Informationen nur verschlüsselt und authentisiert übertragen werden und dass eventuelle Manipulationen nicht zu verbergen sind. Moderne Sicherheitsmechanismen basierend auf kryptographischen Algorithmen und Protokollen, ermöglichen Geheimhaltung, Manipulationssicherheit und Authentisierung, und sind somit in der Lage, die wesentlichsten Herausforderungen zur Kommunikationssicherheit im Automobilbereich zu lösen. Der unkontrollierte Eingriff in die Busse eines Fahrzeugs lässt sich durch eine Reihe von Maßnahmen verhindern. Nachfolgend werden drei elementare Methoden zur Kommunikationssicherheit in Fahrzeugnetzen kurz erläutert.

4.1 Steuergeräteauthentisierung

Die Authentisierung aller Sender ist notwendig, um sicherzustellen, dass nur zulässige Steuergeräte in der Lage sind innerhalb der Fahrzeugbusse miteinander zu kommunizieren. Unautorisierte Nachrichten können dann gesondert behandelt oder direkt verworfen werden. Um sich als neuer gültiger Sender gegenüber dem *Gateway* verifizieren zu können, benötigt jedes Steuergerät ein beglaubigtes Zertifikat. Dieses Zertifikat besteht aus der eindeutigen Identifikationsnummer ID, dem öffentlichen Schlüssel PK und den verschiedenen Berechtigungen $Auth$ des Steuergeräts. Das *Gateway* wiederum, hält geschützt eine Liste öffentlicher Schlüssel aller für das jeweilige Fahrzeug zulässiger OEM (*original equipment manufacturer*). Das Zertifikat

[1] $f \geq n/3$, wobei n = Anzahl existierender FlexRay Knoten. Weitere Informationen in [WL88]

eines Steuergerätes wird mit dem geheimen Schlüssel SK_{OEM} vom OEM signiert, welches so durch das *Gateway* mit dem jeweiligen öffentlichen Schlüssel PK_{OEM} des OEM wieder verifiziert werden kann. Konnte ein Steuergerät erfolgreich authentisiert werden, kann es wie in Tabelle 6 ersichtlich, zur Liste der gültige Steuergeräte hinzugefügt werden.

Authentisierung	
1.$Verify(Sig, PK_{OEM})$	`Verifiziere` Sig `mit dem öffentlichen Schlüssel` PK_{OEM} `des OEM`
2.$ID, PK, Auth$	`Sichere das Zertifikat des Steuergerätes nach erfolgreicher Prüfung`
2.$C = E_{PK}(K_i)$	`Sende verschlüsselt den symmetrischen Busschlüssel` K_i

Tabelle 6: *Steuergeräteauthentisierung*

4.2 Verschlüsselte Datenübertragung

Ein wesentlicher Schritt zur Verbesserung der Kommunikationssicherheit im Automobil ist die Verschlüsselung aller zu übertragender Steuergerätenachrichten. Aufgrund der besonderen technischen Beschränkungen automobiler Kommunikation (Rechenleistung, Zeit, etc.) entspricht die Kombination aus symmetrischer und asymmetrischer Verschlüsselung am ehesten den Bedürfnissen nach angemessener Sicherheit und möglichst geringen Leistungsanforderungen. Während zur Absicherung der internen *Broadcast*-Buskommunikation schnelle und effiziente symmetrische Algorithmen zum Einsatz kommen, werden asymmetrische Verfahren zur notwendigen Schlüsselverteilung eingesetzt.

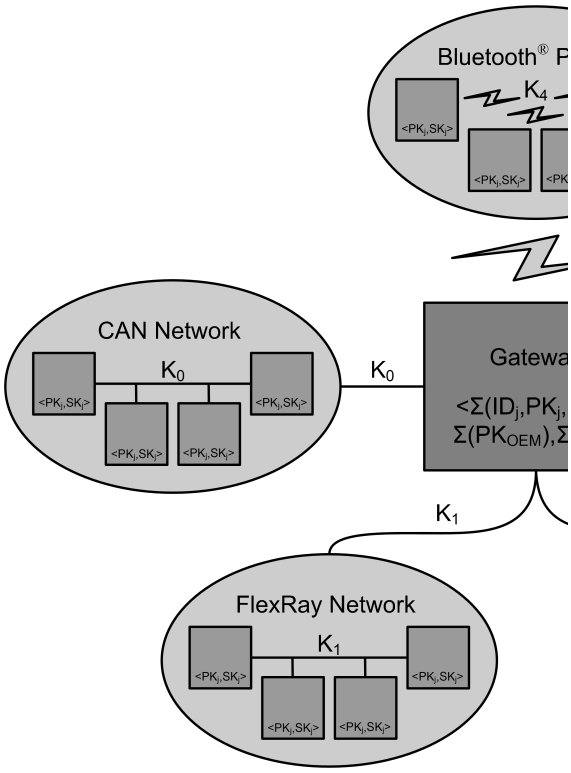

Abbildung 1: *Sichere Fahrzeugkommunikation*

In der Beispielimplementierung in Abbildung 1 verbindet ein zentrales *Supergateway* alle existierenden Bussysteme miteinander und steuert exklusiv jegliche busübergreifende Kommunikation. Dieses *Gateway* verfügt über einen manipulationssicheren (*tamper-resistant*) Speicherbereich um die verwendeten Schlüssel sowie die Liste aller gültigen Steuergeräte zusammen mit

ihren jeweiligen Zertifikaten sicher aufzubewahren. Im Beispiel besitzt jedes erfolgreich authentisierte Steuergerät den gemeinsamen symmetrischen Busschlüssel K_i, seinen öffentlichen und privaten Schlüssel PK_j beziehungsweise SK_j sowie den öffentlichen Schlüssel des *Gateways* PK_G. Das *Gateway* wiederum besitzt neben den Zertifikaten aller gültigen Steuergeräte, auch deren öffentliche Schlüssel PK_j, ihre jeweiligen Sendeberechtigungen $Auth_j$ sowie für die schnelle busübergreifende Kommunikation, alle internen symmetrischen Busschlüssel K_i. Werden nun sämtliche Busnachrichten mit dem jeweiligen Busschlüssel K_i verschlüsselt, sind nur noch Steuergeräte welche über ein gültiges K_i verfügen in der Lage diese Nachrichten zu entschlüsseln und weiter zu verarbeiten. Um die Sicherheit noch weiter zu erhöhen, so dass beispielsweise das Auslesen des gemeinsamen Busschlüssels aus gültigen Steuergeräten zum Einbringen manipulierter Steuergeräte erschwert wird, können alle Busschlüssel zusätzlich periodisch durch das *Gateway* erneuert werden. Tabelle 7 erläutert den Ablauf zum Senden einer Nachricht, welcher optional auch noch die digitale Signatur S_M des Senders enthält, um zusätzlich die Unversehrheit (*integrity*) der Nachricht sowie die Senderauthentisierung zu realisieren.

Senden	
1.$C_1 = Encrypt(M, K_i)$	Verschlüssele Nachricht M mit dem symmetrischen Schlüssel K_i
2.$S_M = Sign(C_1, SK_j)$	Signiere C_1 mit dem geheimen Schlüssel SK_j
3.$C = C_1 \| S_M$	Sende C bestehend aus C_1 und S_M

Tabelle 7: *Gesichertes Versenden von Nachrichten*

Tabelle 8 zeigt den Ablauf beim Empfang einer verschlüsselten Nachricht C durch ein Steuergerät oder das *Gateway*. Während businterne Steuergeräte nur den symmetrischen Teil der Nachricht C_1 entschlüsseln, kann das *Gateway* zusätzlich die optional angehängte Signatur S_M verwenden, um besser differenzierte Firewallregeln auf Steuergerätebene durchzusetzen zu können.

Empfang	
1.$M = Decrypt(C_1, K_i)$	Entschlüssele C_1 zur Nachricht M mit dem symmetrischen Schlüssel K_i
2.$Verify(S_M, PK_j)$	Verifiziere S_M mit dem öffentlichen Schlüssel PK_j (nur Gateway)
3.$Target \in Auth_j$	Leite M ins Zielnetz, falls Berechtigungen $Auth_j$ dies erlauben (nur Gateway)

Tabelle 8: *Gesicherter Empfang von Nachrichten*

4.3 Gateway Firewall

Eine weitere entscheidende Maßnahme zur Kommunikationssicherheit im Fahrzeug, ist die Umsetzung eines geeigneten Zugangskontrollmechanismus. Werden von den sendenden Steuergeräten digitale Signaturen verwendet, basieren die Regeln der *Gateway Firewall* auf den jeweiligen Berechtigungen der einzelnen Steuergeräte. Folglich sind nur noch Steuergeräte mit den notwendigen Berechtigungen in der Lage, Nachrichten auch in hoch sicherheitskritische Bussysteme zu versenden. Ist der Einsatz digitaler Signaturen nicht möglich, können die Regeln zur Zugangskontrolle nur aufgrund der Berechtigungen der jeweiligen Subnetze aufgestellt werden. Dabei sollten Steuergeräte aus untergeordneten LIN- oder MOST-Bussen prinzipiell nicht in der Lage sein, Nachrichten in die sicherheitskritischen CAN- oder FlexRay-Busse zu versenden. Darüber hinaus sind durch die *Gateway Firewall* alle Diagnosefunktionen, welche zur Kontrolle in der Werkstatt oder während der Produktion verwendet werden, im normalen Fahrbetrieb zu unterbinden sowie alle vorhandenen Diagnoseschnittstellen zu deaktivieren.

5 Zusammenfassung und Ausblick

In dieser Arbeit wurde ein Überblick aktueller und zukünftiger automobiler Kommunikationssysteme hinsichtlich ihrer Kommunikationssicherheit gegeben. Es wurden potenzielle Gefahren und mögliche Ansätze zur Lösung beschrieben.

Es ist zu erwarten, dass Multimediabussysteme und drahtlose Kommunikationsschnittstellen bald in den meisten modernen Fahrzeugen vorhanden sein werden. Wie schon heute beispielsweise im Internet ersichtlich, sind gezielte böswillige Angriffe eine ernstzunehmende und vor allem reale Gefahr. Nichtsdestotrotz erfordert der Einsatz komplexer kryptographischer Methoden von den meisten Steuergeräten zusätzliche Rechenleistung und Funktionalität, welche heute den meisten noch nicht ausreichend zur Verfügung steht. Zukünftige Fahrzeugsysteme und automobilbezogene Geschäftsmodelle erfordern jedoch umfassende und leistungsfähige Methoden zur Absicherung der Fahrzeugkommunikation, so dass entsprechend notwendige technische, organisatorische und finanzielle Aufwendungen schon heute zu berücksichtigen sind.

Literatur

[An98] R.J. Anderson. On the Security of Digital Tachographs. In *Lecture Notes in Computer Science, Vol. 1485, 1998, pp. 111+.*

[BSI03] Bundesamt für Sicherheit in der Informationstechnik. Bluetooth - Gefährdungen und Sicherheitsmaßnahmen. In `www.bsi.de/literat/doc/bluetooth/bluetooth.pdf`, *2003.*

[Do02] T. Dohmke. Bussysteme im Automobil CAN, FlexRay und MOST. In *Entwicklung verteilter eingebetteter Systeme, TU Berlin, March 2002.*

[He02] H. Heinecke, A. Schedl, J. Berwanger, M. Peller, V. Nieten, R. Belschner, B. Hedenetz, P. Lohrmann und C. Bracklo. FlexRay - ein Kommunikationssystem für das Automobil der Zukunft. In *Elektronik Automotive 09/2002.*

[JS01] M. Jakobsson, S. Wetzel. Security Weaknesses in Bluetooth. In *Lecture Notes in Computer Science, Vol. 220, 2001, pp. 176+.*

[Kr02] R. Kraus. Ein Bus für alle Fälle. In *Elektronik Automotive 01/2002.*

[Pa03] C. Paar. Eingebettete Sicherheit im Automobil. In *Konferenz „Embedded Security in Cars (ESCAR)“, Köln, November 2003.*

[Pl02] M. Plankensteiner. Sicherheit beim Bremsen und Lenken. In *Elektronik Automotive 09/2002.*

[Po01] S. Poledna, G. Stöger, R. Schlatterbeck, M. Niedersüß. Sicherheit auf vier Rädern. In *Elektronik Automotive 10/2001.*

[Ra02] M. Randt. Bussysteme im Automobil. In *ECT Workshop Augsburg, 2002.*

[RT03] B. Rucha, G. Teepe. LIN - Local Interconnect Network. In *Elektronik Automotive 01/2003.*

[We02] U. Weinmann. Anforderungen und Chancen automobilgerechter Softwareentwicklung. In *3. EUROFORUM-Fachkonferenz, Stuttgart, July 2002.*

[WL88] J.L. Welch, N. Lynch. A new fault-tolerant algorithm for clock synchronization. In *Information and Computation, Vol. 77, No. 1, April 1988. pp. 1 - 36.*

[Ast03] stake Security Consulting Inc. Webseite, 2003. www.atstake.com/events_news/press_mentions/press_mentions_2003.html.

[BaP03] Computer traps Thailand's Finance Minister Suchart. Webseite, May 19, 2003. www.bangkokpost.com.

[Cab04] F-Secure Virus Description: Bluetooth worm Cabir. Webseite, 2004. www.f-secure.com/v-descs/cabir.shtml.

[LIN04] LIN Consortium. Webseite, 2004. www.lin-subbus.de.

[BC04] BOSCH CAN. Webseite, 2004. www.can.bosch.com.

[CIA04] CAN in Automation. Webseite, 2004. www.can-cia.org.

[FL04] FlexRay Group. Webseite, 2004. www.flexray.com.

[MO04] MOST Cooperation. Webseite, 2004. www.mostnet.org.

[Mos04] Mosen Automobilelektronik Webseite, 2004. www.tachoteam.de.

[Spg04] Handyviren: Der Ernstfall wird wahrscheinlicher. Webseite, 2004. www.spiegel.de/netzwelt/technologie/0,1518,310953,00.html.

[VI04] Vector Informatik. Webseite, 2004. www.vector-informatik.de.