Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Ausarbeitung AW1

Stephan Phieler

Sicherheit in Echtzeit-Ethernet-Netzwerken im Automotivkontext

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Motivation

In einem Automobilnetzwerk gibt es heutzutage eine Vielzahl an zu übertragenen Informationen. Viele dieser Informationen müssen aus verschiedensten Gründen geschützt werden (vgl. Koscher u. a., 2010). Rechtliche Interessen, die Geheimhaltung von Herstellerinformationen, die Sicherung von kritischen Informationen und die Privatsphäre der Benutzer sind ein paar Beispiele. All diese Daten und Informationen werden zur Zeit über ein heterogenes Netzwerk, bestehend aus verschiedensten Feldbussen, wie MOST (vgl. MOST Cooperation), CAN (vgl. Robert Bosch GmbH), LIN (vgl. LIN-Administration) oder Flexray (FlexRay Consortium), verteilt (vgl. Nolte u. a., 2005). Somit entsteht ein komplexes Gesamtsystem, welches technologieübergreifend geschützt werden muss.

Die Informationen können dabei unkritisch sein, wie Daten eines Videostreams bei denen ein Informationsverlust oder eine zu große Verzögerung keine sicherheitsrelevanten Auswirkungen auf das System hat oder aber kritisch, mit teilweise sehr kurzen Antwortzeiten, wie bei einer Brake-by-Wire-Lösung. Dabei ist nicht ausgeschlossen, dass kritische und unkritische Informationen zusammenhängen. Löst etwa der Airbag eines Automobils aus, werden kritisch eingestufte Informationen versendet. Zudem werden nach dem Auslösen meist auch die Türen entriegelt, wobei unkritische Informationen versendet werden (vgl. Koscher u. a., 2010).

Auch der Bandbreitenbedarf steigt kontinuierlich. Immer mehr Fahrassistenzsysteme und Steuergeräte, mit neuer Sensorik und Aktorik, kommen im Automobil zum Einsatz. Und auch die Infotainmentanlage verursacht durch Video- und Musikstreaming ein hohes Datenaufkommen, welches in Zukunft durch die Integration des Internets noch zunehmen wird. Dazu kommen weitere Technologien wie die Car-to-Car (C2C)- oder Car-to-Environment (C2E)-Kommunikation.

Um diese Probleme in den Griff zu bekommen, wird von einigen Forschungsgruppen, die in Kapitel 2.3 Konferenzen und Arbeitsgruppen auf Seite 4 vorgestellt werden, die Einführung von Ethernet als einheitliche Kommunikationsplattform untersucht. Dabei wird einerseits die Auflösung des heterogenen Netzwerkes durch den Einsatz von Ethernet als Kommunikations-Backbone angestrebt, um somit die Komplexität des heterogenen Netzes zu verringern und andererseits wird damit dem Bedarf an Bandbreite nachgekommen, wie in Abbildung 1.1 dargestellt. Ethernet bietet sich durch seinen hohen Bekanntheitsgrad und seiner hohen Bandbreite, von bis zu 100Gb/s (vgl. IEEE Computer Society, 2012) für den zukünftigen Einsatz im Automobil an. Der Bekanntheitsgrad wirkt sich dabei sowohl positiv, als auch negativ aus, da es zwar viele existierende Sicherheitskonzepte gibt, aber auch die bestehenden Sicherheitslücken bekannt sind. Ethernet 802.3 hat zudem den Nachteil, dass es keine harten Echtzeiteigenschaften besitzt, was den Einsatz zur Übertragung von kritischem Datenverkehr ausschließt.

Eine Lösung bietet die Firma TTTech an, welche mit Time-Triggered-Ethernet (TTE) eine Echtzeiterweiterung für das Standard-Ethernet 802.3 entwickelt hat (vgl. TTTech Computer-

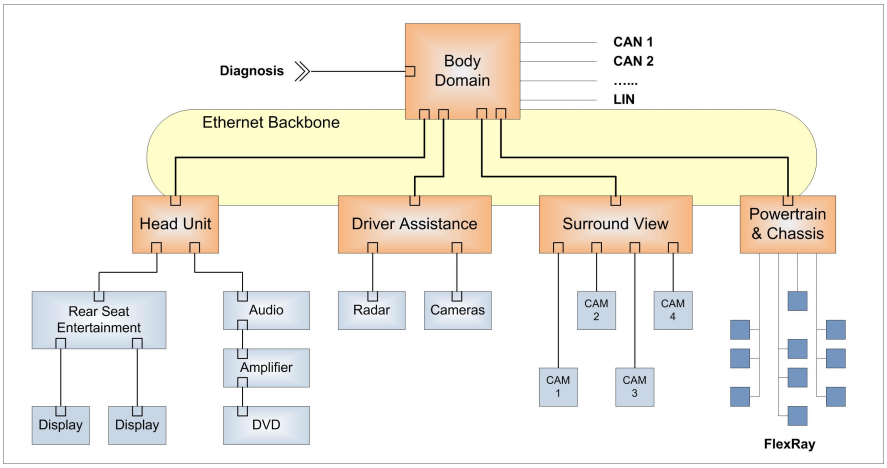

Abbildung 1.1: Ethernet als Backbone im Automobilnetzwerk (Quelle: Hank u. a., 2012)

technik AG). Diese ist vollständig kompatibel zum 802.3-Standard und ist seit 2011 selbst ein eingetragener Standard (vgl. SAE AS6802, 2011).

Auch die Forschungsgruppe Communication over Realtime Ethernet (CoRE), in dessen Kontext diese Arbeit entsteht, untersucht die Einführung von Ethernet und TTE als Kommunikations-Backbone im Automobil. Dazu wurde bereits ein Prototyp einer Steer-by-Wire-Lösung entwickelt, an dem gezeigt wird, welche Möglichkeiten diese Technologie bietet. Zusätzlich werden mithilfe von Computer-Simulationen weitere Tests durchgeführt.

Ziel dieser Ausarbeitung ist es eine Übersicht über die aktuelle Forschung zum Thema Security in Echtzeit-Ethernet-Netzwerken im Automotivekontext zu erstellen. Dazu werden in Kapitel 2 Grundbegriffe der Informationssicherheit erläutert, sowie ein Überblick über Normen und Standards gegeben. Weiter werden die aktuellen Forschungsgruppen und wichtige Konferenzen vorgestellt. Kapitel 3 zeigt die Themenschwerpunkte der Forschungsgruppen auf. Abschließend wird in Kapitel 4 eine Zusammenfassung gegeben.

2 Überblick

In diesem Kapitel wird ein Überblick über die aktuelle Forschung zum Thema Security in Ethernet-Netzwerken im Automotivekontext gegeben. Dazu wird zuerst erläutert, was Security ist und wie diese in Informationssystemen definiert wird. Anschließend werden Standards und Normen beschrieben, nach welchen Informationssysteme konzipiert und entwickelt werden müssen. Abschließend werden aktuelle und kürzlich abgeschlossene Forschungsprojekte, Arbeitsgruppen sowie Konferenzen und Tagungen vorgestellt.

2.1 Informationssicherheit

Unter Informations- oder Datensicherheit versteht man die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen bzw. Daten.

Vertraulichkeit

Unter Vertraulichkeit der Daten versteht man, dass die abgelegten oder gerade übertragenden Daten nur von berechtigten Benutzern genutzt und verändert werden dürfen.

Integrität

Unter Integrität versteht man, dass Daten nicht unbemerkt verändert werden dürfen.

Verfügbarkeit

Die Verfügbarkeit von Daten sagt aus, dass diese immer innerhalb einer definierten Zeit zugänglich sein müssen.

IT-Sicherheit

IT-Sicherheit beschreibt alle technischen Maßnahmen zur Einhaltung der Ziele der Informationssicherheit. Sie beinhaltet dabei alle potentiell gefährdeten Systeme. Dies betrifft in diesem Kontext alle Netzwerkkomponenten, einschließlich Hard- und Software. Für die Einhaltung und Umsetzung der IT-Sicherheit gibt es nationale und internationale Standards und Normen.

2.2 Standards und Normen

Die nachfolgenden Standards und Normen befassen sich mit der Umsetzung der Sicherheitsanforderungen in der Informationssicherheit.

DIN NIA-01-27

Die in Deutschland geltenden Normen zur IT-Sicherheit, werden von der DIN NIA-01-27 festgelegt. Diese beschreibt unter anderem die Anforderungen an IT-Sicherheitssysteme, -komponenten und -produkten. Weiter beinhaltet sie Normen zu kryptographischen und nicht kryptographischen Sicherheitstechniken, sowie Leitfäden für das Management von IT-Sicherheit und Kriterien für die Evaluierung und Zertifizierung der Sicherheit von IT-Systemen, -Komponenten und -Produkten. Die erarbeiteten Normen fließen auch in die internationale ISO/IEC 2700X-Norm ein (vgl. DIN NIA-01-27:2010, 2010).

ISO/IEC 2700X

Diese Norm spezifiziert die Anforderungen für Aufbau, Implementierung, Betrieb, Überwachung, Überprüfung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter den Bedürfnissen einer Organisation, wobei alle Arten von Organisationen erfasst werden (vgl. ISO/IEC 27001:2005, 2005). Sie ist in mehrere Themengebiete aufgeteilt, die von der groben Beschreibung (vgl. ISO/IEC 27001:2005, 2005) bis hin zu speziellen Szenarien (vgl. ISO/IEC 27033-3:2010, 2010) reichen.

ISO 26262

ISO 26262 beschreibt die Vorgehensweisen in Planung und Produktion sicherheitsrelevanter elektrischer und/oder elektronischer (E/E) Systeme in Personenkraftwagen bis einschließlich 3500Kg. Wie ISO/IEC 2700X ist auch ISO 26262 in mehrere Teile separiert. Diese umfassen vom Managment, der Konzeption bis hin zur Produktion und Service, alle Bereiche in denen eine funktionale Sicherheit gefordert ist (vgl. ISO 26262-1:2011, 2011).

2.3 Konferenzen und Arbeitsgruppen

Nachfolgend wird ein Überblick über Konferenzen und Arbeitsgruppen gegeben, die sich unter anderem mit Security in Ethernet-Netzwerken im Automotivebereich befassen oder befasst haben. In Tabelle 2.1 sind dazu die aktuellen Projekte und Arbeitsgruppen mit ihren Themenschwerpunkten zu sehen. Tabelle 2.2 zeigt aktuelle Konferenzen und Tagungen, die als Schwerpunkt das Thema Security im Automotivekontext haben oder sich allgemein mit Security in der IT beschäftigen.

Viele der Arbeitsgruppen aus Tabelle 2.1 befassen sich mit der Integration des Internet Protocol (IP) und Ethernet 802.3, sowie WLAN 802.11 und GSM/GPRS/HSDPA (vgl. simTD Konsortium). Damit soll, wie eingangs beschrieben, dem steigenden Bandbreitenbedarf im Auto entgegengekommen werden, sowie eine C2C/C2E Kommunikation ermöglicht werden. Auch der Einsatz von TTE fand bei einigen Projekten Beachtung (vgl. Bello, 2011).

Arbeitsgruppe	Laufzeit	Themengebiete und Ziele
EVITA *E-safety vehicle intrusion protected applications*	2008-2011	C2C-Kommunikation, Konzipierung von Hardwarekomponenten zur sicheren C2C-Kommunikation, (vgl. Fraunhofer Institute for Secure Information Technology)
SEIS *Sicherheit in Eingebetteten IP-basierten Systemen*	2009-2012	Einführung von IP im Automobil, Einführung von Sicherheitskonzepten für die IP-Kommunikation, (vgl. Innovationsallianz Automobilelektronik E ENOVA)
simTD *Sichere Intelligente Mobilität Testfeld Deutschland*	2008-2013	C2C-/C2E-Kommunikation, Sichere und intelligente Mobilität, (vgl. simTD Konsortium)
PRESERVE *Preparing Secure Vehicle-to-X Communication Systems*	2011-2014	C2C-/C2E-Kommunikation, Entwicklung einer günstigen und skalierbaren Sicherheitssystemarchitektur, (vgl. CORDIS)
AUTOSAR *AUTomotive Open System ARchitecture*	2005-heute	Gemeinsame Entwicklung von E/E-Standards im Automobil, (vgl. AUTOSAR Development Cooperation)

Tabelle 2.1: Arbeitsgruppen

Konferenz/Tagung	Themengebiet
ESCAR *Embedded Security in Cars*	Sicherheits- & Risikobetrachtung im Automobilnetzwerk
VDI/VW - AS *Verein Deutscher Ingenieure/Volkswagen 29th-Automotive Security*	Sichere Vernetzung von Automobilen
Automotive *Safety & Security*	Zuverlässigkeit und Sicherheit softwarebasierter Funktionen
IEEE Symposium on Security and Privacy	Sicherheit und Privatspähre in der IT
SAFECOMP *The International Conference on Computer Safety, Reliability and Security*	Computer Sicherheit und Zuverlässigkeit

Tabelle 2.2: Konferenzen und Tagungen

3 Security in Echtzeit-Ethernet-Netzwerken

In diesem Kapitel werden die speziellen Anforderungen an Security in Echtzeit-Ethernet-Netzwerken im Automotivebereich beschrieben. Dazu werden zuerst die Stakeholder identifiziert und ihre Motivationen aufgezeigt. Da Ethernet und IP bekannte Technonologien sind, werden anschließend Lösungsansätze gezeigt, die auch im Automotivebereich Anwendung finden oder dafür geeignet sind.

3.1 Besonderheiten im Automobilnetzwerk

Das Netzwerk in einem Automobil unterliegt einigen Besonderheiten, welche nachfolgend erläutert werden.

Lebenszyklus

Laut dem Kraftfahrt-Bundesamt liegt das Durchschnittsalter von den 60,8 Millionen in Deutschland angemeldeten Fahrzeugen bei 8,7 Jahren (vgl. Kraftfahrt Bundesamt, 2013). Davon sind knapp eine halbe Million Fahrzeuge 30 Jahre oder älter. Die Nutzungsdauer reicht somit von wenigen Jahren bis hin zu mehreren Dekaden.

Mobiles Echtzeitnetzwerk

Die Position eines Automobils kann sich ständig ändern. Das Netzwerk kann dabei immer wieder mit anderen unbekannten Netzwerken interagieren. Zudem unterliegt es teilweise harten Echtzeiteigenschaften.

Limitierte Ressourcen

Steuergeräte, Sensoren und Aktoren verfügen nur über begrenzte und teilweise nur wenige Ressourcen.

Sicherheitskritisches System

Das Automobil ist ein sicherheitskritisches System. Ein Ausfall oder eine Funktionsstörung kann für die Insassen lebensgefährlich sein.

Stakeholder

Es gibt viele potentielle Angreifer, die die Security-Maßnahmen umgehen oder ausschalten wollen. Die Motivationen sind dabei sehr unterschiedlich. Angefangen bei einfachen Autodieben, die nur die Absicht haben das Auto zu stehlen, bis hin zum eigenen Besitzer der das Auto seinen Vorlieben anpassen oder Beschränkungen außer Kraft setzen möchte. Auch Mitarbeiter der Hersteller oder Zulieferer haben ein Interesse daran Security-Maßnahmen in bestimmten Fällen zu umgehen. So wäre es für sie durchaus wünschenswert Backdoors zu haben, die sie z.B. als Druckmittel gegen Entlassung einsetzen können, oder um sich jederzeit Zugang zu einem Netzwerk verschaffen zu können, sollte es von einem Angreifer kompromittiert worden sein (vgl. Hofmann und Kasseckert, 2011). Organisationen und Regierungen sind vielleicht daran interessiert Securtiy-Maßnahmen, die zum Schutz der Privatsphäre dienen, zu umgehen, um Nutzerverhalten zu analysieren oder Spionage zu betreiben. Und auch Terroristen bilden eine Gruppe von potentiellen Angreifern.

Es gibt aber auch eine große Gruppe von Personen, die an der Aufrechterhaltung der Sicherheit des Boardnetzwerkes interessiert sind. Hersteller und Zulieferer könnten bei bekannten Sicherheitsmängeln Vertrauen bei den Kunden verlieren. Ein Fahrzeugbesitzer möchte natürlich zu jeder Zeit die Kontrolle über sein Fahrzeug behalten.

Die Arten der Motivation reichen vom einzelnen De-/Aktivieren von Funktionen oder von Sperren, bis zur vollen Kompromittierung des Fahrzeugnetzwerkes.

3.2 Maßnahmen

Die Maßnahmen zum Schutz der Kommunikation, zum Aufrechterhalten der Privatsphäre und die Analyse der Auswirkungen einer unzureichenenden oder umgangenen Security, lassen sich in die drei Kategorien Prevention, Detection und Consequences einordnen.

3.2.1 Prevention

Prevention beschreibt die Maßnahmen von Security, die getroffen werden um die Informationssicherheit zu gewährleisten. Sie kann dabei auf verschiedenen Schichten im Netzwerk betrieben werden. Nachfolgend werden bekannte Security-Maßnahmen anhand des OSI-Modells vorgestellt, die auch im Automotivebereich Anwendung finden oder dessen Einsatz diskutiert wird.

Schicht 1 - Physical-Layer

Um den physischen Zugang zum Netzwerk zu verhindern, werden bauliche Maßnahmen umgesetzt, die es erschweren oder verhindern fremde Netzwerkkomponenten zu integrieren oder bestehende zu entfernen und auszutauschen. Nur über speziell ausgewiesene Schnittstellen, wie der Diagnoseschnittstelle oder einer Multimediaschnittstelle, ist so der Zugang zum Netzwerk erlaubt.

Schicht 2 - Data-Link-Layer

Um eine fehlerfreie und sichere Übertragung der Daten auf Schicht 2 zu gewährleisten, kann Media Access Control Security (MACsec) verwendet werden. Es sichert die Integrität und Vertrauenswürdigkeit der Daten und stellt Mittel zur Authentifizierung bereit (vgl. IEEE Computer Society, 2006). Da es nicht an das Internet Protocol gebunden ist, kann es auch dort eingesetzt werden, wo andere Protokolle zum Einsatz kommen. Ein weiterer Vorteil ist, dass es vollständig in Hardware implementiert werden kann und sich somit auch für den Einsatz in eingebetteten Systemen eignet. Allerdings wird durch MACsec nur eine Punkt-zu-Punkt-Verbindung und keine End-zu-End-Kommunikation geschützt. Die Daten sind, selbst wenn alle Teilnehmer MACsec unterstützen, während sie sich beim jeweiligen Teilnehmer befinden, ungeschützt (vgl. Hofmann und Kasseckert, 2011).

Schicht 3 - Network-Layer

Wie eingangs beschrieben, treiben einige Forschungsgruppen die Einführung von Ethernet und IP als Kommunikationsnetz im Automobil voran. Für IPv4 und IPv6 gibt es mit Internet Protocol Security (IPsec) eine Erweiterung, die es erlaubt den Header und den Payload des IP-Paketes zu verschlüsseln (vgl. Internet Engineering Task Force, 2005). Durch den verschlüsselten Payload kann die Integrität der Daten gewährleistet und durch Authentifizierungsmöglichkeiten die Vertraulichkeit der Daten sichergestellt werden. Darüber hinaus sichert es, anders als MACsec, die komplette Kommunikationsstrecke ab (vgl. Hofmann und Kasseckert, 2011). Dabei ist die Implementierung unabhängig von der Hardware, da sie komplett in Software umgesetzt wird. Auch die Verschlüsselungsalgorithmen können je nach Einsatzgebiet passend ausgetauscht werden, was mit Blick auf die Limitierung der Ressourcen von eingebetteten Systemen wichtig sein kann.

Schicht 4-7 - Transport-Layer/Application-Layer

Um Daten zu schützen, die mithilfe von TCP übertragen werden, kann TLS/SSL eingesetzt werden (vgl. Dierks und Rescorla, 2008) (vgl. Dierks und Allen, 1999). TCP kann beispielsweise zum Streamen eines Films verwendet werden. Wie bei IPsec können selbstgewählte Verschlüsselungsalgorithmen verwendet werden und die Implementierung erfolgt ausschließlich in Software. Ein Nachteil von TLS/SSL ist die Anfälligkeit gegen DoS-Attacken.

3.2.2 Detection

Unter Detection versteht man das Erkennen der Ausnutzung von Sicherheitslücken. Sollten Preventionsmaßnahmen fehlgeschlagen sein, muss ein Angriff rechtzeitig erkannt und wenn möglich vereitelt werden. Dazu lassen sich Techniken auf verschiedenen Ebenen anwenden.

Network-Monitoring

Ein Monitoring des Datenverkehrs auf Netzwerkebene kann einen Angriff auf das Netzwerk sichtbar machen. Dazu kann man, unter anderem durch Paket-Sniffing, die Bandbreitennutzung

beobachten, um festzustellen wie sich der anfallende Datenverkehr über die Zeit verändert. Sniffing erlaubt aber auch auf den Inhalt von Paketen zuzugreifen, um diesen auf Anomalien zu untersuchen. Da im Automobil ein Switched-Ethernet eingesetzt werden soll und somit nicht alle Datenpakete an alle Ports eines Switches weitergeleitet werden, muss man entweder mehrere Sniffer im Netzwerk verteilen, oder sich auf bestimmte Verbindungen konzentrieren, wie beispielsweise den Schnittstellen zur Kommunikation mit den externen Geräten.

System-Monitoring

Man kann ein Monitoring auch direkt auf einer Systemkomponente, wie einem Steuergerät oder einer reinen Überwachungskomponente realisieren, um einen Angriff zu entdecken. Dazu kann das Verhalten einer Software und das Starten von Diensten durch Logs festgehalten und analysiert werden. Systemkomponenten mit einem Betriebssystem können Aktivitäten des Root-Benutzers überwachen oder Änderungen am Dateisystem feststellen und ggf. unterbinden oder zumindest aufzeichnen. Die Systemsoftware selbst muss eingehende Daten auf ihre Plausabilität überprüfen. Dies kann auch für gerichtliche Auseinandersetzungen im Falle eines Unfalls von Bedeutung sein.

3.2.3 Consequences

Consequences zeigen mögliche Auswirkungen der Ausnutzung von Sicherheitslücken und ggf. Ansätze zu deren Beseitigung. Eine Analyse eines aktuellen Fahrzeuges aus dem Jahr 2009 hat gezeigt, dass selbst vorhandene Sicherheitsmechanismen nicht oder nur unzureichend genutzt werden (vgl. Koscher u. a., 2010). Zudem wurde gezeigt, dass auch Daten, die als unkritisch eingestuft werden, durchaus mit kritischen Daten in Zusammenhang stehen können, wie das eingangs beschriebene entriegeln der Türen nach dem Auslösen der Airbags. Es wurden weiterhin Szenarien gezeigt, die das Leben der Fahrzeuginsassen in hohem Maße gefährden und rein durch unkritische Daten herbeizuführen waren. So war es möglich bestimmte Dienste, wie die Scheibenwischanlage oder das Autoradio, an die Geschwindigkeit des Fahrzeuges zu koppeln, so dass ab einer bestimmten Geschwindigkeit das Radio auf die volle Lautstärke eingestellt wurde, was auf einer Autobahn kritisch sein kann.

3.2.4 Zusammenfassung

Es gibt keine Maßnahme, die allein ausreichend ist, um die gesamte Netzwerkinfrastruktur zu schützen. Nur die Kombination aus verschiedenen Maßnahmen kann sicherstellen, dass die Daten vor Missbrauch sicher sind. Ein Problem, welches sich im Automobilbereich zeigt, ist das Beheben von Sicherheitslücken und das Aktualisieren von Sicherheitsmechanismen. Werden neue Sicherheitslücken entdeckt, oder sogar ausgenutzt, muss schnell dafür gesorgt werden, dass diese beseitigt werden. Dies könnte bei Software zum großen Teil über das Funknetz geschehen, sollte das Problem aber die Hardware sein, so kann dies einen hohen Kostenaufwand und einen Imageschaden für den Hersteller bedeuten. Außerdem kann nicht gewährleistet werden, dass alle Fahrzeuge regelmäßig in die Werkstatt kommen.

4 Zusammenfassung und Ausblick

Als Erstes erfolgt eine kurze Zusammenfassung der Arbeit und anschließend ein Ausblick auf die kommenden Aufgaben.

4.1 Zusammenfassung

Mit dieser ersten Analyse, der derzeitigen Situation in Forschung und Entwicklung, wurde festgestellt, dass ein Automobilnetzwerk eigene spezielle Anforderung besitzt. Vor allem die Deckung des Bandbreitenbedarfs, die Auflösung des heterogenen Gesamtsystems und die Vernetzung mit der Umwelt, sind Schwerpunkte der aktuellen Forschung. Neue Technologien, wie C2C/C2E oder autonomes Fahren, machen die Anwesenheit von Security im Boardnetzwerk unabdingbar. Dabei sollten nicht nur die kritischen Daten geschützt werden, sondern auch unkritische. Die Motivationen, Security-Maßnahmen auszuhebeln, ist durch eine Vielzahl an potentiellen Angreifern sehr vielfältig. Von einfachen Anpassungen, wie dem Aktivieren oder Deaktivieren von Funktionen oder Sperren, bis hin zur kompletten Übernahme der Kontrolle des Fahrzeuges durch Unauthorisierte.

Um die Probleme des Bandbreitenbedarfs zu lösen und die Auflösung des heterogenen Gesamtsystems zu erreichen, schlagen viele Forschungsgruppen den Einsatz von Ethernet im Automobil vor. Da Ethernet selbst nicht echtzeitfähig ist, müssen Erweiterungen, wie das TTE eingesetzt werden. Auch die Forschungsgruppe CoRE untersucht den Einsatz von TTE mithilfe eines Prototypen und anhand von Simulationen. Dabei kann in Bezug auf Security, auf einen großen Pool an Security-Mechanismen zugegriffen werden. Es ist aber auch wichtig, sich mit den Schwächen der Security-Mechanismen auseinander zu setzen.

4.2 Ausblick

Das Themengebiet Detection wird für eine spätere Umsetzung von C2C/C2E-Kommunikation sehr wichtig sein. Das Vortäuschen von Gefahrensituationen durch fehlerhafte oder kompromittierte Fahrzeuge oder Verkehrsüberwachungssysteme kann zu erheblichen Schäden führen. Daher müssen Daten, die von außerhalb kommen, auf ihre Plausabilität überprüft werden. Dabei helfen die eigenen Sensordaten, sowie die Daten weiterer Verkehrsteilnehmer. Es ist in diesem Kontext aber vorallem wichtig zu definieren, wann welche Daten plausibel sind oder nicht.

Es ist daher eine schnelle und richtige Bewertung der Daten erforderlich. Somit gilt es zu untersuchen, wie eine solche Bewertung von Daten aussehen und wie diese effektiv umgesetzt werden kann.

Abkürzungsverzeichnis

C2C Car-to-Car

C2E Car-to-Environment

CAN Controller Area Network

CoRE Communication over Realtime Ethernet

DoS Denial of Service

E/E elektrisch/elektronisch

GPRS General Packet Radio Service

GSM Global System for Mobile Communications

HSDPA High Speed Downlink Packet Access

IP Internet Protocol

IPsec Internet Protocol Security

LIN Local Interconnect Network

MACsec Media Access Control Security

MOST Media Oriented Systems Transport

SSL Secure Sockets Layer

TCP Transmission Control Protocol

TLS Transport Layer Security

TTE Time-Triggered-Ethernet

Literaturverzeichnis

[AUTOSAR Development Cooperation] AUTOSAR Development Cooperation: *AUTomotive Open System ARchitecture*. – URL http://www.autosar.org

[Bello 2011] Bello, Lucia L.: The case for ethernet in automotive communications. In: *SIGBED Rev.* 8 (2011), Dezember, Nr. 4, S. 7–15. – URL http://doi.acm.org/10.1145/2095256.2095257. – ISSN 1551-3688

[CORDIS] CORDIS: *Preparing Secure Vehicle-to-X Communication Systems*. – URL http://www.preserve-project.eu. – Zugriffsdatum: 2013-05-26

[Dierks und Allen 1999] Dierks, T. ; Allen, C.: *RFC 2246 - The TLS Protocol Version 1.0*. IETF (Veranst.), Januar 1999. – URL http://www.ietf.org/rfc/rfc2246.txt. – Zugriffsdatum: 2013-07-19

[Dierks und Rescorla 2008] Dierks, T. ; Rescorla, E.: *RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008. – URL http://tools.ietf.org/html/rfc5246. – Zugriffsdatum: 2013-07-19

[DIN NIA-01-27:2010 2010] : *IT-Sicherheitsverfahren*. März 2010. – URL http://www.nia.din.de/cmd?level=tpl-artikel&languageid=de&cmstextid=sicherheitsverfahren. – Zugriffsdatum: 2013-05

[FlexRay Consortium] FlexRay Consortium: *FlexRay*. – URL http://flexray.com/. – Zugriffsdatum: 2012-09-26

[Fraunhofer Institute for Secure Information Technology] Fraunhofer Institute for Secure Information Technology: *E-safety vehicle intrusion protected applications*. – URL http://www.evita-project.org. – Zugriffsdatum: 2013-03-27

[Hank u. a. 2012] Hank, Peter ; Suermann, Thomas ; Mueller, Steffen: *Ethernet backbone in domain architecture*. 2012. – URL http://itersnews.com/wp-content/uploads/2012/08/Fig-4-Backbone-Architecture.jpg. – Zugriffsdatum: 2013-07-17

[Hofmann und Kasseckert 2011] Hofmann, Stefan ; Kasseckert, Rudolf: Safeguards for the Internal Communication of IP-Based Transmission and Cross-Connect Systems. In: *Photonic Networks; 12. ITG Symposium; Proceedings of*, 2011, S. 1–8

[IEEE Computer Society 2006] IEEE Computer Society: *IEEE Standard 802.1 AE: Media Access Control (MAC) Security*. August 2006. – URL https://standards.ieee.org/findstds/standard/802.1AE-2006.html. – Zugriffsdatum: 2013-07-18

[IEEE Computer Society 2012] IEEE Computer Society: *IEEE 802.3 Standard for Ethernet*. 2012. – URL http://standards.ieee.org/getieee802/download/802.3-2012_section1.pdf. – Zugriffsdatum: 2013-07-19

[Innovationsallianz Automobilelektronik E ENOVA] Innovationsallianz Automobilelektronik E ENOVA: *SEIS - Sicherheit in Eingebetteten IP-basierten Systemen*. – URL http://www.strategiekreis-elektromobilitaet.de/public/projekte/seis. – Zugriffsdatum: 2013-05-06

[Internet Engineering Task Force 2005] Internet Engineering Task Force: *Security Architecture for the Internet Protocol*. RFC 4301 (Proposed Standard). Dezember 2005. – URL http://www.ietf.org/rfc/rfc4301.txt

[ISO 26262-1:2011 2011] : *Road vehicles – Functional safety – Part 1: Vocabulary*. November 2011. – URL http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43464. – Zugriffsdatum: 2013-05

[ISO/IEC 27001:2005 2005] : *Information technology – Security techniques – Information security management systems – Requirements*. Juli 2005. – URL http://www.iso.org/iso/catalogue_detail?csnumber=42103. – Zugriffsdatum: 2013-05

[ISO/IEC 27033-3:2010 2010] : *Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues*. April 2010. – URL http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51582. – Zugriffsdatum: 2013-05-11

[Koscher u. a. 2010] Koscher, K. ; Czeskis, A. ; Roesner, F. ; Patel, S. ; Kohno, T. ; Checkoway, S. ; McCoy, D. ; Kantor, B. ; Anderson, D. ; Shacham, H. ; Savage, S.: Experimental Security Analysis of a Modern Automobile. In: *Security and Privacy (SP), 2010 IEEE Symposium on*, 2010, S. 447–462. – ISSN 1081-6011

[Kraftfahrt Bundesamt 2013] Kraftfahrt Bundesamt: *Der Fahrzeugbestand am 1. Januar 2013*. KBA (Veranst.), Januar 2013. – URL http://www.kba.de/cln_031/nn_125398/DE/Statistik/Fahrzeuge/Bestand/Kurzbericht/2013__b__text.html. – Zugriffsdatum: 2013-07-17

[LIN-Administration] LIN-Administration: *Local Interconnect Network*. – URL http://www.lin-subbus.org/. – Zugriffsdatum: 2011-01-06

[MOST Cooperation] MOST Cooperation: *Media Oriented Systems Transport*. – URL http://www.mostcooperation.com/. – Zugriffsdatum: 2011-01-06

[Nolte u. a. 2005] Nolte, T. ; Hansson, H. ; Bello, L.L.: Automotive communications-past, current and future. In: *Emerging Technologies and Factory Automation, 2005. ETFA 2005. 10th IEEE Conference on* Bd. 1, 2005, S. 8 pp.–992

[Robert Bosch GmbH] Robert Bosch GmbH: *Controller Area Network*. – URL http://www.semiconductors.bosch.de/. – Zugriffsdatum: 2011-02-03

[SAE AS6802 2011] : *Time-Triggered Ethernet*. 2011. – URL http://standards.sae.org/as6802/. – Zugriffsdatum: 2013-06-14

[simTD Konsortium] simTD Konsortium: *Sichere Intelligente Mobilität Testfeld Deutschland*. – URL www.simtd.de. – Zugriffsdatum: 2013-06-02

[TTTech Computertechnik AG] TTTech Computertechnik AG: *Time-Triggered-Ethernet*. – URL http://www.tttech.com. – Zugriffsdatum: 2011-01-17