Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Seminar

Stephan Phieler

Informationssicherheit in Echtzeit-Ethernet Bordnetzen

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BE Best Effort

BIOS Basic Input/ Output System

CAN Controller Area Network

DoS Denial of Service

ICV Integrity Check Value

IPSec Internet Protocol Security

LIN Local Interconnect Network

MAC Message Authentication Code

MOST Media Oriented Systems Transport Bus

PCF Protocol Control Frame

PTP Precision Time Protocol

RC Rate-Constrained

SA Security Association

SMV Secure Membership Vector

SPoF Single Point of Failure

TDMA Time Division Multiple Access

TT Time-Triggered

TTE Time-Triggered-Ethernet

TÜV Technischer Überwachungsverein

1. Motivation und Problemstellung

Das Auto entwickelt sich immer mehr von einem mechanisch zentrierten zu einem elektronisch zentrierten Medium. Elektronische Assistenzsysteme, die mit GPS, Ultraschall und Kameras arbeiten sowie ein Infotainmentsystem gehören heute in vielen Fahrzeugen schon zur Serienausstattung. Hinzu kommen Systeme die mit Radar, Funk und Laserscannern ausgestattet sind. Die Vernetzung dieser Systeme wird durch Feldbusse wie das Controller Area Network (CAN), das Local Interconnect Network (LIN), den Media Oriented Systems Transport Bus (MOST) oder Flexray realisiert, welche ein heterogenes Netzwerk aufspannen und jeweils speziellen Aufgabendomänen zugeordnet sind. Die Anforderungen an die Höhe der Bandbreite steigen durch den Einsatz von Elektronik immer weiter, und die eingesetzten Feldbusse stoßen an ihre Grenzen (vgl. Nolte u. a., 2005).

Eine Alternative, um die heterogene Struktur aufzulösen und dem Bedarf an Bandbreite gerecht zu werden, ist der Einsatz von Ethernet 802.3. In Ethernet 802.3 können allerdings keine Aussagen über die Latenz, den Jitter und die Zustellung von Nachrichten getroffen werden. Dies ist aber essentiell für das Bordnetz, da auch kritische Nachrichten mit harten Echtzeitanforderungen kommuniziert werden. Daher ist eine Erweiterung nötig, welche diese Anforderungen erfüllt. Hierzu passt das von der TU Wien entwickelte und heute von der Firma TTTech Computertechnik AG vertriebene Time-Triggered-Ethernet (TTE) (vgl. SAE AS6802, 2011; Steinbach, 2008; Steinbach u. a., 2010).

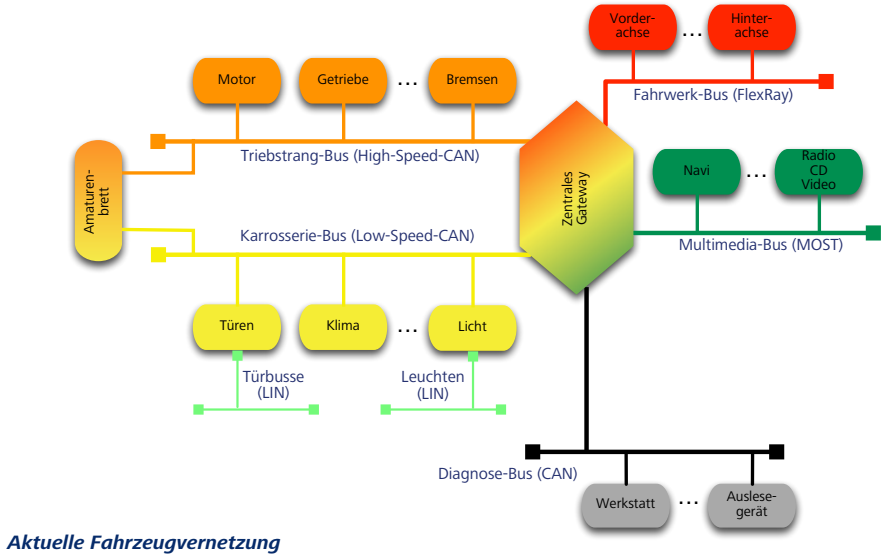

Abbildung 1: Bordnetz

Durch die verwendete Sensorik wird auch ein großer Teil an sensiblen Daten erhoben, welche auch für Dritte interessant sind. So kann es eine Autoversicherung interessieren ob das Fahrzeug ihres Kunden oft in unsicheren Gegenden genutzt wird oder ob der Kunde eher einen aggressiven Fahrstil hat, um so die Beiträge genauer anzupassen. Zudem werden Funktionen,

AW 1	Sicherheit in Echtzeit-Ethernet-Netzwerken im Automotivkontext
AW 2	Authentifizierungsverfahren in Echtzeit-Ethernet-Netzwerken im Automotivkontext
Projekt 1	Sichere Synchronisation in Echtzeit-Ethernet Bordnetzen
Projekt 2	Sichere Kommunikation in Echtzeit-Ethernet Bordnetzen
Masterarbeit	Konzept einer Sicherheitsarchitektur für ein Echtzeit-Ethernet Bordnetz

Tabelle 1: Entwicklung Masterarbeit

wie die Abriegelung der Motordrehzahl, elektronisch eingestellt und können zentral über die Diagnoseschnittstelle oder manipulierte Hardware (z.B. Chiptuning) außer Kraft gesetzt werden. Somit besteht heute und zukünftig ein großer Bedarf an Informationssicherheit.

In Fahrzeugen der heutigen Generation sind rudimentäre Sicherheitsmaßnahmen für das Bordnetz und deren Teilnehmern enthalten, welche aber nur selten oder gar nicht eingesetzt werden (vgl. Wolf, 2009; Henniger u. a., 2009; Koscher u. a., 2010; Checkoway u. a., 2011; Tillich und Wójcik, 2012; Studnia u. a., 2013a,b). Eine Besonderheit des Bordnetzes ist die große Anzahl an Stackholdern, wie z.B. dem Autodieb, dem Besitzer (De-/ Aktivieren von Funktionen), dem Hersteller (Überwachung und Manipulation) oder Organisationen (Überwachung und Manipulation). Eine weitere Besonderheit ist es, dass später nur begrenzter oder gar kein Zugriff auf das Bordnetz möglich ist, da nicht jedes Land Institutionen wie den Technischer Überwachungsverein (TÜV) hat oder eine Werkstattuntersuchung vorschreibt. Spät oder gar nicht festgestellte Sicherheitslücken können so für die betroffenen Firmen sehr teuer werden. Daher ist es notwendig von Anfang an ein Sicherheitskonzept, parallel zur Entwicklung eines neuen Bordnetzes, zu erstellen. Dazu müssen auch lokale Gesetze und Normen, wie die ISO2700X in Deutschland, einbezogen werden.

Das Ziel meiner Masterarbeit ist der Entwurf eines Sicherheitskonzeptes, welches auf das zukünftige, auf Echtzeit-Ethernet basierende, Bordnetz anwendbar ist. Dazu wurde bereits untersucht, welche bestehenden Konzepte adaptiert werden können und welche Sicherheitsanforderungen an das zukünftige Bordnetz gestellt werden, um so die Schwerpunkte der Arbeit festlegen zu können. Als grobes Konzept wird hierzu die Arbeit von Wasicek (2011) verwendet. Dieser teilt das Sicherheitsmanagement in 3 Phasen ein. Phase 1 ist die sichere Initialisierung des Netzwerkes und wird in Abschnitt 3.1 beschrieben. In Abschnitt 3.2 wird Phase 2, welche sich mit der Sicherung der Synchronisation befasst, dargestellt. Phase 3 beschäftigt sich in Abschnitt 3.3 mit der Absicherung der kritischen Datenkommunikation. Tabelle 1 zeigt die einzelnen Punkte der Masterarbeit.

2. AS6802 - Time-Triggered Ethernet

TTE ist eine Echtzeiterweiterung für das Ethernet 802.3 und ist vollständig zu diesem kompatibel (vgl. SAE AS6802, 2011). Es unterstützt die Kommunikation von zeitkritischen und

zeitunkritischen Daten über ein Medium. Das Protokoll basiert auf dem Time Division Multiple Access (TDMA)-Ansatz, bei dem feste Zeitpunkte definiert werden, in denen bestimmte Nachrichten gesendet oder empfangen werden dürfen. Die Zeitpunkte werden zyklisch wiederholt abgearbeitet. Zudem muss es eine zeitliche Synchronisation geben, damit alle Teilnehmer die richtigen Zeitpunkte benutzen. Es ist somit möglich Aussagen über die Latenz und den Jitter zu treffen. Die Konfiguration des Netzwerkes wird vor dem Betrieb statisch festgelegt.

2.1. Grundlagen und Funktionsweise

Es gibt in TTE drei Nachrichtenklassen für die Nutzdatenkommunikation sowie eine Nachrichtenklasse für die Synchronisation. Die zeitgesteuerten Time-Triggered (TT)-Nachrichten haben die höchste Priorität und werden zu vorher bestimmten Zeitpunkten abgearbeitet. Somit ist gewährleistet, dass sie immer die gleichen Sende- und Empfangszeitpunkte besitzen und ausreichend Bandbreite vorhanden ist. Rate-Constrained (RC)-Nachrichten bilden die zweite Klasse. Sie treten ereignisgesteuert auf und können untereinander priorisiert werden. Auch ihnen wird eine ausreichende Bandbreite reserviert, da zur Konfigurationszeit bekannt ist, wo und in welcher Regelmäßigkeit sie auftreten werden. Die letzte Klasse für Nutzdaten, Best Effort (BE)-Nachrichten, entsprechen den Standard-Ethernet 802.3-Nachrichten.

2.2. Synchronisation

TTE beinhaltet bereits ein Protokoll zur Synchronisation der Netzwerkteilnehmer. Sein Vorteil liegt darin, dass es sehr ressourcenschonend ist, da nur eine weitere Nachrichtenklasse für die Synchronisation hinzugefügt wird und pro Zyklus nur eine Nachricht von jedem Teilnehmer verschickt werden muss. Ein alternatives und sehr bekanntes Protokoll ist das PTP. Dieses ist zwar weniger ressourcenschonend als das in TTE integrierte Protokoll, bietet dafür aber eine sehr hohe Genauigkeit (vgl. IEEE, 2008). Nachfolgend wird eine Zusammenfassung der Funktionsweisen beider Protokolle gegeben.

2.2.1. Synchronisation in TTE

Für die Synchronisation in TTE werden Protocol Control Frames (PCFs) verwendet. Diese werden normalerweise am Anfang eines Zyklus gesendet und empfangen und haben eine höhere Priorität als TT-Nachrichten. Sie treten, wie RC-Nachrichten, eventgesteuert auf, da es zum Startzeitpunkt noch kein synchronisiertes Netzwerk gibt und zeitgesteuerte Nachrichten nicht versendet oder empfangen werden können.

Jeder Teilnehmer der das TTE unterstützt hat eine bestimmte Rolle im Synchronisationsprozess. Er ist entweder ein Synchronisation-Client, der weiter keine aktive Funktion in der Synchronisation einnimmt, ein Synchronisation-Master oder ein Compression-Master. Alle Rollen werden in der Konfigurationsphase, welche vor dem Betrieb stattfindet, statisch zugeordnet. Die Synchronisation-Master schicken, wie in Bild 2 zu sehen ist, ihre lokale Zeit an einen Compression-Master. Dieser sammelt über einen bestimmten Zeitraum Nachrichten ein und führt anschließend auf den übermittelten Zeiten eine Durchschnittsberechnung aus, um eine neue Zeit zu bestimmen. Diese sendet er dann an alle Synchronisation-Master und

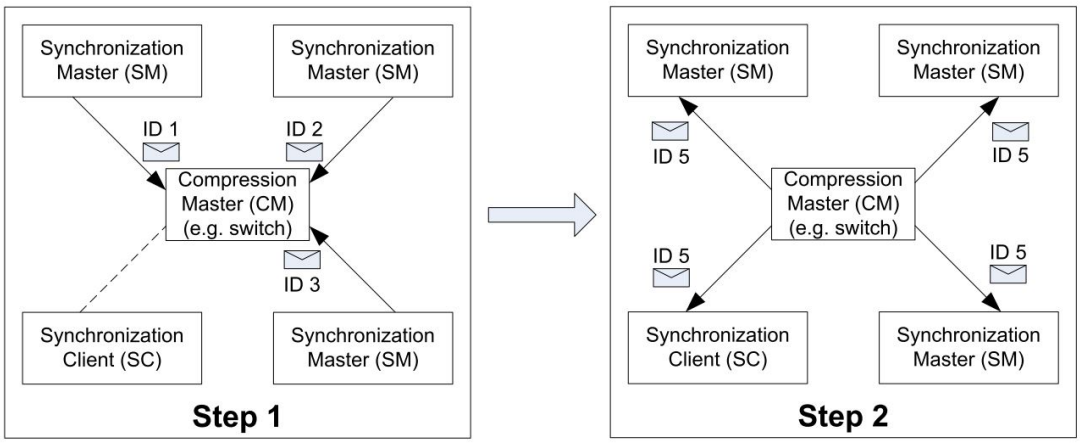

Abbildung 2: TTE Synchronisationsprozess (Quelle: SAE AS6802 (2011))

Synchronisation-Clients, die daraufhin ihre lokale Zeit anpassen. Alle Teilnehmer leiten die Nachrichten vom Compression-Master solange weiter, bis sie einen Endknoten erreicht haben.

2.2.2. IEEE 1588-2008 - Precision Time Protocol

Das PTP wurde im Jahr 2002 standardisiert und im Jahr 2008 überarbeitet. Nachfolgend wird sich immer auf die überarbeitete Fassung bezogen. PTP basiert auf dem Master-/ Slave-Konzept. Wie in Bild 3 und 4 zu sehen ist, sendet der Master seine lokale Zeit mit Hilfe einer Sync-Nachricht, an einen Slave. Um die round-trip time zu ermitteln, sendet der Slave zuerst eine Delay-Request-Nachricht an den Master. Daraufhin sendet der Master eine Delay-Response-Nachricht, wieder mit seiner lokalen clock time, an den Slave. Da im PTP davon ausgegangen wird, dass Hin- und Rückweg des Paketes gleich lang sind und sich diese Werte über die Zeit nur sehr langsam ändern, kann nun mit der Formel 2 die round-trip time bestimmt werden. Um eine noch höhere Genauigkeit zu erreichen, kann nach der Sync-Nachricht noch eine Follow-Up-Nachricht vom Master gesendet werden, in der der genaue Absendezeitpunkt der Sync-Nachricht festgehalten ist. Somit kann eine theoretische Genauigkeit von $2^{-16}ns$ erreicht werden. Die neue lokale clock time kann mit der Formel 3 bestimmt werden.

$$\text{delay} = \frac{(t_2 - t_1) + (t_4 - t_3)}{2} \tag{1}$$

$$\text{round-trip time} = 2 * \text{delay} \tag{2}$$

$$\text{clock time} = delay + t_1 \tag{3}$$

Anders als bei Synchronisationsprotokoll von TTE wird der Master im PTP dynamisch gewählt. Dies geschiet mit Hilfe des Best-Master-Clock-Algorithmus, bei dem der Node zum Master gewählt wird, welcher die beste Zeitgüte hat. Jeder Node publiziert dafür die Genauigkeit

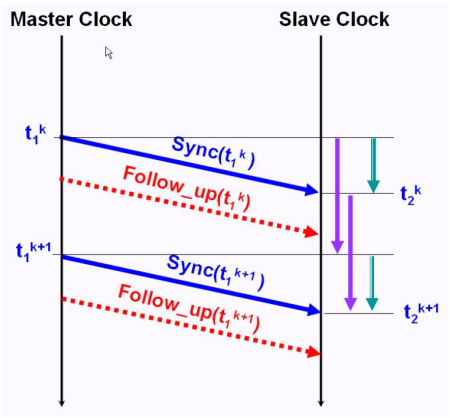

Abbildung 3: PTP Syntonization
(Quelle: Weibel (2009))

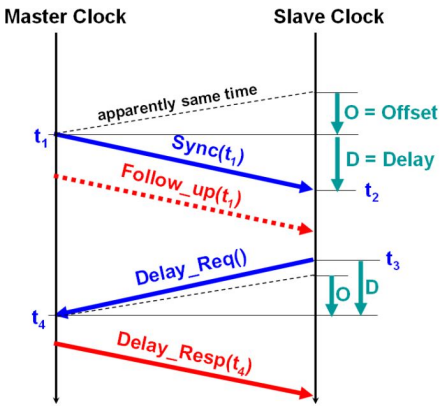

Abbildung 4: PTP Offset und delay
(Quelle: Weibel (2009))

seiner lokalen Uhr im Netzwerk. Der Node mit der genausten oder der topologisch besten Uhr gewinnt. Sollten mehrere Uhren die gleiche Qualität haben, wird der Node mit der höchsten MAC-Adresse gewählt. Dabei wird nicht überprüft, ob der Node die Güte überhaupt besitzt.

2.3. Sicherheitskonzept

TTE ist ein fehlertolerantes Kommunikationsprotokoll, welches aber keine Regeln zur Nutzung und Integration von Sicherheitsfunktionen und zum Schutz der Informationssicherheit bestimmt hat (vgl. Steiner, 2013). Zudem muss davon ausgegangen werden, dass versucht werden wird, das TTE-Netzwerk oder die Teilnehmer, aktiv zu kompromittieren, wenn dieses im Auto eingesetzt werden sollte. Ethernet bietet durch seinen hohen Bekanntheitsgrad auch für Laien einen leichten Einstieg in das Bordnetz (vgl. Torchinsky, 2014). Es sollte also vor dem Produktiveinsatz in einem Auto ein Sicherheitskonzept erstellt werden. Dabei bietet TTE schon durch seine statische Struktur einige sicherheitsrelevante Funktionen. So ist es nicht möglich beliebige zeitgesteuerte Nachrichten zu versenden. Nur solche Nachrichten sind zulässig, die vorher in der statischen Konfiguration festgelegt wurden. Alle anderen Nachrichten werden beim Empfänger sofort verworfen. Auch das Nutzen von freien Ports an einem Switch ist nicht möglich, da auch hier nur die in der statischen Konfiguration festgelegten Ports genutzt werden können. Trotzdem sind weitere Maßnahmen nötig (vgl. Steiner, 2013).

Vorallem die Firma TTTech und die TU Wien (vgl. Skopik u. a., 2012) forschen in diesem Gebiet, um das TTE-Protokoll sicherer zu machen. Auch diese Arbeit befasst sich damit, ein Sicherheitskonzept für das TTE zu erarbeiten. Dazu werden im Abschnitt 3 die drei Hauptpunkte nach Wasicek (2011) genauer erläutert und beschrieben welche Herausforderungen und Risiken es zu beachten gibt.

3. Sicherheitskonzept für ein Bordnetzwerk

In diesem Kapitel werden die 3 Phasen des Konzeptes nach Wasicek (2011) beschrieben und wie diese auf das Bordnetz im Auto angewendet werden können. Zudem wird ein Einblick in die Herangehensweise der Analyse und Erstellung des Sicherheitskonzepts gegeben.

Bedrohungs- und Risikoanalyse

Welche Bereiche eines Systems Schutzbedarf aufweisen, kann mit einer Bedrohungs- und einer Risikoanalyse festgestellt werden. Sie helfen Schwachpunkte zu erkennen, welche für einen erfolgreichen Angriff ausgenutzt werden können. Als Erstes müssen dafür die Gefahren und möglichen Ziele eines Angreifers identifiziert werden. Dabei können manche Ziele Teilziele eines anderen Ziels sein. Anschließend wird nach Schwachstellen gesucht, die zu einem erfolgreichen Angriff ausgenutzt werden können. Eine Methode um Schwachstellen und Angriffsmöglichkeiten zu ermitteln, ist das Erstellen von Bedrohungsbäume. Für jedes determinierte Ziel wird ein eigener Bedrohungsbaum erstellt. Somit kann auch die Wahrscheinlichkeit eines Angriffes abgeschätzt werden. Muss viel Aufwand betrieben werden und ist der Nutzen dabei gering, kann davon ausgegangen werden, dass ein Angriff eher unwahrscheinlich ist. Zur besseren Visualisierung können auch Programme wie SecureITree[1] oder SeaMonster[2] eingesetzt werden. Anschließend wird das Risiko für das System bewertet. Um das Risiko abschätzen zu können, kann die Formel 4 angewandt werden. Die Eintrittswahrscheinlichkeit wird im Bereich zwischen 0 bis 1 angegeben. Wobei 0 für unwahrscheinlich und 1 für wahrscheinlich steht. Der Schaden ist ein abstrakter Wert, welcher z.B. den finanziellen Schaden darstellen kann.

$$Risiko = Eintrittswahrscheinlichkeit * Schaden \tag{4}$$

Die erfassten Informationen zu Bedrohungen, Schwachstellen und Risiken bilden die Sicherheitsanforderungen an das System. Anhand derer anschließend die Gegenmaßnahmen erarbeitet werden.

Tools zu Bedrohungsbäumen?

3.1. Sichere Initialisierung des Bordnetzwerks

Da sich dieser Bereich der Sicherheit auf die Hardware und Software der Netzwerkteilnehmer bezieht und sich mit diesem Thema in anderen Forschungsgruppen bereits beschäftigt wird, wie z.B. EVITA (2011) und EscryptII (2012), wird hier nur ein kurzer Überblick gegeben.

Eine sichere Initialisierung der Teilnehmer ist die Basis für ein sicheres Netzwerk. Das Ziel der sicheren Initialisierung ist die Sicherstellung der Authentizität und der Integrität der Firmware. Diese umfasst die ausführbare Software, zum Beispiel das Betriebssystem, und die Konfiguration. Beim Start eines Computersystems wird eine Bootsequenz ausgeführt die mehreren Schritten unterliegt. Als Erstes wird das Basic Input/ Output System (BIOS)

[1] https://www.amenaza.com/
[2] http://sourceforge.net/projects/seamonster/

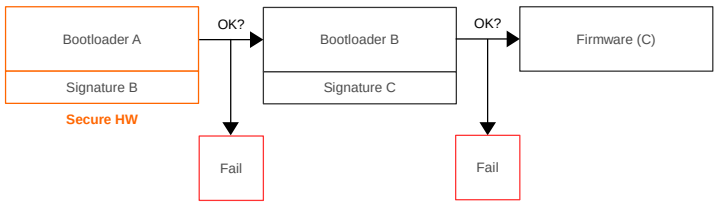

Abbildung 5: Sichere Initialisierung der Firmware

geladen, welches vom Hersteller signiert wurde und damit als vertrauenswürdig gilt. Dies wird durch mehrere unabhängige Integritätschecks realisiert (vgl. Arbaugh, 1997). Dabei muss darauf geachtet werden, dass das BIOS in einem, für Dritte unzugänglichen, gesicherten Speicher abgelegt wird. Anschließend wird die Firmware geladen, welche nicht unbedingt vom Hersteller bereitgestellt worden sein muss. Zum Beispiel kann diese auch von externen Zulieferern kommen, welche vorgefertigte Hardware nutzen.

Daher ist es notwendig eine Funktion einzubinden, welche die Authentizität und die Integrität der Firmware überprüft. Eine Möglichkeit ist es, einen weiteren Prozess nach dem Start des BIOS auszuführen, welcher dann die eigentliche Firmware lädt (vgl. Wasicek, 2011), was in Bild 5 veranschaulicht wurde. Dieser wird durch das BIOS geladen und hat die Aufgabe die Integrität der Firmware zu überprüfen. Auf dieser Basis können die ausgeführten Programme und die Konfigurationen als vertrauenswürdig eingestuft werden (vgl. Arbaugh, 1997). Zusätzlich wird vorgeschlagen einen externen Monitor einzurichten, der die Firmware und deren Prozesse überwacht. Prozesse deren Signatur nicht korrekt oder nicht bekannt ist, können so nicht ausgeführt werden. Eine weitere Möglichkeit ist es, dass alle Prozesse in einer virtualisierten Umgebung ausgeführt werden. Somit können sie keinen Einfluß auf andere Prozesse ausüben oder das Betriebssystem schädigen.

3.2. Sichere Synchronisation des Bordnetzwerks

Nach der sicheren Initialisierung muss die zeitliche Synchronität der Teilnehmer hergestellt werden. Erst dann ist es möglich TT-Nachrichten zu versenden oder zu empfangen. Das TTE hat, wie eingangs beschrieben, ein eigenes Zeitsynchronisationsprotokoll. Es ist aber auch möglich ein anderes Protokoll zu verwenden, z.B. das PTP. Nachfolgend werden die Sicherheitsanforderungen aufgezeigt, welche an das PTP und an die Zeitsynchronisation von TTE gestellt werden und Schwachstellen sowie Lösungsansätze erläutern.

3.2.1. Bedrohungs- und Risikoanalyse

Ein Angriff auf die Zeitsynchronisation ist schon deshalb kritisch, weil ohne sie die Übertragung von zeitgesteuertem Datenverkehr nicht möglich ist. Daher ist es notwendig diese abzusichern.

Das Hauptziel bei einem Angriff auf die Synchronisation ist es, die Kontrolle über die Zeit zu erlangen (vgl. Treytl und Hirschler, 2009; Treytl u. a., 2006), zum Beispiel um die Synchronisation so zu stören, dass der Betrieb eines Nodes oder des gesamten Netzwerks nicht mehr möglich ist (Denial of Service (DoS)). Dazu hat ein Angreifer mehrere Möglichkeiten. Zum einen kann er versuchen falsche Informationen zu verbreiten. Dies kann er dadurch erreichen, dass er bestehende Nachrichten manipuliert oder eigene Nachrichten publiziert. Zum anderen kann er Informationen zurückhalten oder löschen. Dies sind alles Gefahren und Angriffe die auf die Kommunikationsinfrastruktur gerichtet sind. Die Synchronisationsprotokolle selbst bieten aber auch Angriffspunkte. Diese gilt es in diesem Teil der Arbeit zu erfassen.

3.2.2. Fallbeispiel Best-Master-Clock-Algorithmus

Ein ausgewiesenes Angriffsziel ist der Best-Master-Clock-Algorithmus von PTP (vgl. Treytl und Hirschler, 2009). Ein fehlerhafter oder kompromittierter Node kann veranlassen, dass eine neue Abstimmung über den Master initialisiert wird. In dieser Zeit ist kein TDMA möglich und somit können auch keine TT-Nachrichten kommuniziert werden. Ein Bedrohungsbaum zu diesem Beispiel ist in Anhang A in Bild 6 zu sehen. In dem Fallbeispiel wird gezeigt, wie ein Angreifer versucht, den Best-Master-Clock-Algorithmus anzustoßen und welche Maßnahmen ergriffen werden können, um ihn daran zu hindern. Da erst einmal keine Sicherheitsmaßnahmen angewandt werden, kann er dieses Ziel leicht erreichen. Er muss sich dazu Zugang zum Netzwerk verschaffen, die Zeitinformation überschreiben und die Nachricht weiterleiten. Diese drei Punkte sind aber voneinander abhängig, was bedeutet, dass dieser Angriff nicht erfolgreich durchführbar ist, wenn ein Punkt nicht erfüllt wird.

Eine Möglichkeit ist, die Wahl erst gar nicht zu ermöglichen, in dem man den Master statisch festlegt (siehe Anhang A Bild 7). Eine andere ist es, nur solche Nodes eine Wahl initiieren zu lassen, welche vorher als vertrauenswürdig deklariert worden sind (siehe Anhang A Bild 8). Haris Isakovic beschreibt in seiner Arbeit „A Secure Global Time Base for Time Triggered Systems“ den Einsatz eines binären Secure Membership Vectors (SMVs) (vgl. Isakovic, 2011). In diesem SMV ist hinterlegt, ob ein Node als vertrauenswürdig eingestuft worden ist oder nicht. Mit jeder Synchronisationsnachricht vom Client an den Master werden zwei Prüfungen durchgeführt. Zuerst wird die Authentizität der Nachricht überprüft, was voraussetzt, dass es ein entsprechendes Authentifizierungsverfahren gibt. Anschließend wird überprüft, ob der Client zum Master synchronisiert ist. Sind beide Prüfungen bestanden, gilt der Node als vertrauenswürdig. Der SMV wird an jede Synchronisationsnachricht vom Master an den Client angehangen. Somit weiß ein Node auch mit welchem anderen Nodes er kommunizieren kann. Je nachdem welches Authentifizierungsverfahren eingesetzt wird, muss gewährleistet werden, dass der Master über genügend Speicher und Rechenkapazität verfügt. Anschließend muss nun noch die Kommunikation unter den Nodes abgesichert werden (siehe Abschnitt 3.3).

3.2.3. Sicherheitsmaßnahmen

In PTPv2 wurde, neben anderen Sicherheitsmaßnahmen zum Schutz der Synchronisation, das Prinzip der Security Associations (SAs) eingeführt, welches auch in der Internet Protocol

Security (IPSec) eingesetzt wird. SAs beinhalten Informationen über die Absicherung der Kommunikation zwischen zwei Nodes. Sie werden dynamisch unter den Nodes gebildet und sind unidirektional. Enthalten sind Informationen zu der eingesetzten Hashfunktion und dem Secret-Key, sowie die Ports und die Adressen des Quell- und des Zielnodes, eine zufällige Lifetime-Id und ein Replay Counter (vgl. IEEE, 2008). Der Sender entscheidet, ob er einen Secret-Key für alle Empfänger verwendet oder für jeden einen eigenen benutzt. Nachrichten die über eine SA übertragen werden, sind mit dem SECURE-Flag gekennzeichnet und enthalten eine Integrity Check Value (ICV) sowie einen AUTHENTICATION TLV[3]. Die ICV ist das Ergebnis der Hashfunktion über der Nachricht mit dem Secret-Key. Nur die Nodes, welche den Secret-Key kennen, können die Informationen verändern und eine neue ICV erzeugen. Aber auch hier wurden Schwachstellen entdeckt. So kann ein Node beliebig viele SAs mit dem immer selben Node erzeugen und so den Node von anderen Aufgaben abhalten (vgl. Treytl und Hirschler, 2009).

3.3. Sichere Kommunikation im Bordnetzwerk

Nachdem die Synchronisation aufgebaut ist, können TT-Nachrichten verschickt und empfangen werden. Da TT-Nachrichten für den Einsatz in kritischen Systemen vorgesehen sind, müssen die Nachrichten abgesichert werden. Die Schutzziele der sicheren Kommunikation für TT-Nachrichten sind Integrität, Vertraulichkeit und Verfügbarkeit (Informationssicherheit). Schwerpunkt der Arbeit ist die Sicherstellung der Integrität von TT-Nachrichten. Um die Integrität der TT-Nachrichten sicherzustellen, muss eine Authentifizierung stattfinden. Ähnlich wie bei der Synchronisation und dem SMV, muss analysiert werden, welche Methoden eingesetzt werden können, so dass die Übertragung nicht negativ beeinflusst wird. Auch hier wird wieder eine Bedrohungs- und Risikoanalyse durchgeführt. Man hat hier aber den Vorteil, durch die hohe Verbreitung von Ethernet, dass viele Bedrohungen, Angriffsziele und Angriffsarten bekannt sind.

3.3.1. Authentifizierung

Es gibt zwei grundlegende Vorgehensweisen eine Nachricht zu authentifizieren. Einmal kann ein Message Authentication Code (MAC) erstellt und der Nachricht hinzugefügt werden. Dabei wird ein Hashwert über die gesamte Nachricht oder über Teile davon gebildet und anschließend der Nachricht angefügt. Da die Hashfunktion für jeden bekannt ist, und damit jeder die Nachricht erstellen hätte können, wird der Hashwert zusammen mit einem geheimen Schlüssel gebildet. Dieser ist nur dem Sender und seinen Empfängern bekannt. Es handelt sich also um eine symmetrische Verschlüsselung. Die zweite Variante ist der Einsatz einer Signatur. Der Hauptunterschied zum MAC-Verfahren liegt darin, das eine asymmetrische Verschlüsselung eingesetzt wird. Der Vorteil des Verfahrens mit einem MAC ist, dass die Bildung des Hashwertes schnell ist. Einen Nachteil gibt es, wenn ein Schlüssel für alle Nodes verwendet wird. Dann kann ein kompromittierter Node das gesamte System beeinflussen (Single Point of Failure (SPoF)). Werden allerdings für alle Kommunikationspfade eigene

[3] TLV steht für type, length, value nach IEEE Std 802.1AB

Schlüssel verwendet, müssen die Nodes genügend Kapazität besitzen um diese zu speichern. Das System skaliert dann aber schlecht. Der Vorteil beim Signaturverfahren ist, dass es gut skaliert. Es benötigt aber im Vergleich zum MAC-Verfahren wesentlich mehr Rechenzeit. Dies kann dazu führen, dass es nicht so einfach für die Sicherung von TT-Nachrichten eingesetzt werden kann. Es gilt somit ein Verfahren zu finden, welches im Bordnetz angewandt werden kann.

3.3.2. Weiteres

Zu dem sollten weitere Methodiken, welche zum Schutz beitragen können, in Betracht gezogen werden. Dazu zählen zum Beispiel der Einsatz von Honeypots, Sandboxing, das Monitoring des Systems oder das Bilden von speziellen Sicherheitszonen.

3.4. Risiken

Bei der Konzeption für ein Sicherheitskonzept ist es schwierig vorherzusagen, ob und wie sich die Umsetzung in den Punkten Jitter und Delay auf das Protokoll auswirken. Verwendet man Methodiken die einen negativen Einfluss auf den Synchronisationsprozess haben, kann es sein, dass nur eine schlechte (geringe Genauigkeit) oder gar keine Synchronisation durchführbar ist. Oder TT-Nachrichten werden unkontrollierbar verzögert und können dadurch ihre Deadlines nicht mehr einhalten. Daher ist es wichtig sich mit Personen auszutauschen, die auf diesem Gebiet Erfahrung haben und die Auswirkungen einschätzen können. Man muss auch darauf achten, die Probleme und Lösungen abstrakt genug zu beschreiben, denn es kann sonst vorkommen, dass man jeden Einzelfall mit speziellen Ausnahmeregelungen bedient. Es kann aber auch daran scheitern, dass das Konzept technisch so nicht umsetzbar ist. Zusätzlich sind Gesetze und Normen zu beachten, die von Land zu Land unterschiedlich sein können, denn auch Organisationen und Regierungen haben ein Interesse an den Daten im oder dem Zugang zum Auto, z.B. um Autos ferngesteuert anzuhalten (vgl. Krempl, 2014).

4. Zusammenfassung und Fazit

In heutigen aber auch in zukünftigen Bordnetzen besteht ein Bedarf an Informationssicherheit, denn immer mehr Anwendungen im Auto werden elektronisch realsiert. Viele dieser Anwendungen kommunizieren untereinander und bilden dadurch ein verteiltes System in welchem auch kritische Daten übertragen werden. Daher muss ein Sicherheitkonzept erstellt werden, welches die Daten im Auto schützt. Die hier vorgestellte Vorgehensweise besteht aus drei Phasen. Zuerst die sichere Initialisierung, dann die sichere Synchronisation und als Letztes die sichere Kommunikation. Diese Arbeit befasst sich vorallem mit der zweiten und dritten Phase. Bei der sicheren Synchronisation wird auf die Schwachstellen in der Übertragung von Synchronisationsnachrichten und den Schwachstellen in den Synchronisationsprotokollen eingegangen. Es wird geschaut, wie die Arbeit von Isakovic (2011) auf das Bordnetz abgebildet werden kann, um eine Vertrauensbasis aufzubauen. Die sichere Kommunikation befasst sich mit der Absicherung, im speziellen der Integrität, des zeitgesteuerten Datenverkehrs. Es soll ein

Konzept erarbeitet werden, das eine Authentifizierung von Nachrichten mit hohen zeitlichen Anforderungen realisierbar macht. Zum Abschluss soll ein Gesamtkonzept, basierend auf den Erkenntnissen aus Phase 2 und 3, erstellt werden.

Literatur

[EscryptII 2012] *ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)*, September 2012. – URL http://www.ecrypt.eu.org/documents/D.SPA.20.pdf. – Zugriffsdatum: 12.12.2013

[Arbaugh 1997] Arbaugh, WA: A secure and reliable bootstrap architecture. In: *Secur. Privacy, 1997. ...* (1997), S. 65–71. – URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=601317

[Checkoway u. a. 2011] Checkoway, Stephen ; Mccoy, Damon ; Kantor, Brian ; Anderson, Danny ; Shacham, Hovav ; Savage, Stefan ; Koscher, Karl ; Czeskis, Alexei ; Roesner, Franziska ; Kohno, Tadayoshi: Comprehensive Experimental Analyses of Automotive Attack Surfaces. (2011)

[EVITA 2011] EVITA: *E-safety vehicle intrusion protected applications*. 2011. – URL http://www.evita-project.org. – Zugriffsdatum: 2014-11-27

[Henniger u. a. 2009] Henniger, Olaf ; Apvrille, Ludovic ; Fuchs, Andreas ; Roudier, Yves ; Ruddle, Alastair ; Weyl, Benjamin ; Paristech, Telecom ; Ltci, Cnrs ; Antipolis, Sophia: Security requirements for automotive on-board networks. (2009), S. 641–646. ISBN 9781424453474

[IEEE 2008] IEEE: *1588-2008 - IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*. 2008. – URL http://standards.ieee.org/findstds/standard/1588-2008.html. – Zugriffsdatum: 2014-11-29

[Isakovic 2011] Isakovic, Haris: *A secure global time base for time triggered systems*, Technische Universität Wien, Institut für Technische Informatik, Dissertation, 2011

[Koscher u. a. 2010] Koscher, Karl ; Czeskis, Alexei ; Roesner, Franziska ; Patel, Shwetak ; Kohno, Tadayoshi ; Checkoway, Stephen ; McCoy, Damon ; Kantor, Brian ; Anderson, Danny ; Shacham, Hovav ; Savage, Stefan: Experimental Security Analysis of a Modern Automobile. In: *2010 IEEE Symp. Secur. Priv.* (2010), S. 447–462. – URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5504804. ISBN 978-1-4244-6894-2

[Krempl 2014] Krempl, Stefan: EU-Polizeinetzwerk will Autos ferngesteuert stoppen. (2014). – URL http://www.heise.de/-2098389.html. – Zugriffsdatum: 14.01.2015

[Nolte u. a. 2005] Nolte, T ; Hansson, H ; Bello, LL: Automotive communications-past, current and future. In: *Emerging Technologies and ...* 1 (2005), S. 985–992. – URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1612631. ISBN 078039402X

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

[Skopik u. a. 2012] Skopik, Florian ; Treytl, Albert ; Geven, Arjan ; Hirschler, Bernd: Towards secure time-triggered systems. In: *..., Reliab. Secur.* (2012), S. 1–8. – URL http://link.springer.com/chapter/10.1007/978-3-642-33675-1_33

[Steinbach 2008] Steinbach, Till: *Ethernet als Bus für Echtzeitanwendungen im Automobil.* Dezember 2008. – URL http://users.informatik.haw-hamburg.de/~ubicomp/projekte/master08-09-aw1/steinbach/bericht.pdf. – Zugriffsdatum: 2011-01-08. – Bericht

[Steinbach u. a. 2010] Steinbach, Till ; Korf, Franz ; Schmidt, Thomas C.: Comparing Time-Triggered Ethernet with FlexRay: An Evaluation of Competing Approaches to Real-time for In-Vehicle Networks. In: *8th IEEE Intern. Workshop on Factory Communication Systems.* Piscataway, New Jersey : IEEE Press, Mai 2010, S. 199–202

[Steiner 2013] Steiner, Wilfried: Candidate security solutions for TTEthernet. In: *Digit. Avion. Syst. Conf. (DASC), 2013 ...* (2013), S. 1–10. – URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6712579. ISBN 9781479915385

[Studnia u. a. 2013a] Studnia, Ivan ; Nicomette, Vincent ; Alata, Eric ; Deswarte, Yves: Security of embedded automotive networks : state of the art and a research proposal. (2013)

[Studnia u. a. 2013b] Studnia, Ivan ; Nicomette, Vincent ; Alata, Eric ; Deswarte, Yves ; Kaâniche, Mohamed ; Laarouchi, Youssef ; Toulouse, F: Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks. (2013)

[Tillich und Wójcik 2012] Tillich, Stefan ; Wójcik, M: Security analysis of an open car immobilizer protocol stack. In: *Trust. Syst.* 3 (2012). – URL http://link.springer.com/chapter/10.1007/978-3-642-35371-0_8

[Torchinsky 2014] Torchinsky, Jason: *The Tesla Model S Is Basically A Good Looking IT Department On Wheels.* 2014. – URL goo.gl/9XC7jo. – Zugriffsdatum: 27.11.2014

[Treytl u. a. 2006] Treytl, Albert ; Gaderer, Georg ; Loschmidt, Patrick ; Kerö, N: Investigations on Security Aspects in Clock Synchronized Industrial Ethernet. In: *Proc. Investig. ...* (2006), S. 232–240. – URL http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Investigations+on+Security+Aspects+in+Clock+Synchronized+Industrial+Ethernet#0

[Treytl und Hirschler 2009] Treytl, Albert ; Hirschler, Bernd: Security flaws and workarounds for IEEE 1588 (transparent) clocks. In: *2009 Int. Symp. Precis. Clock Synchronization Meas. Control Commun.* 1588 (2009), Oktober, S. 1–6. – URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5340204. ISBN 978-1-4244-4391-8

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

[Wasicek 2011] Wasicek, A: Security in time-triggered systems. 2011 (2011). – URL http://www.informatik.tuwien.ac.at/dekanat/Kurzfassung-Wasicek.pdf

[Weibel 2009] Weibel, Prof H.: Technology Update on IEEE 1588 : The Second Edition of the High Precision Clock Synchronization Protocol. (2009), S. 1–8

[Wolf 2009] Wolf, Marko: Mehr Sicherheit auf unseren Straßen. (2009), S. 1–8

A. Fallbeispiel A

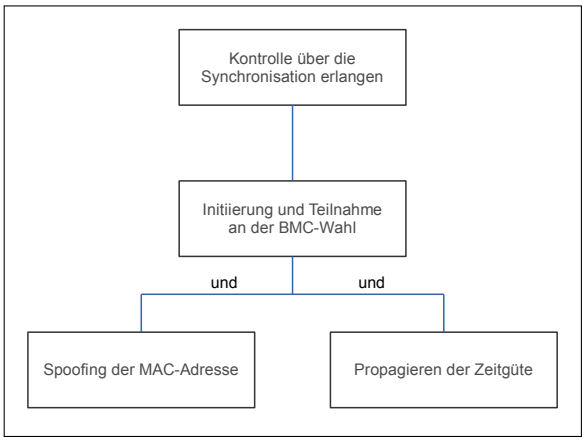

Abbildung 6: Bedrohungsbaum Fallbeispiel Best-Master-Clock-Algorithmus ohne Sicherheit

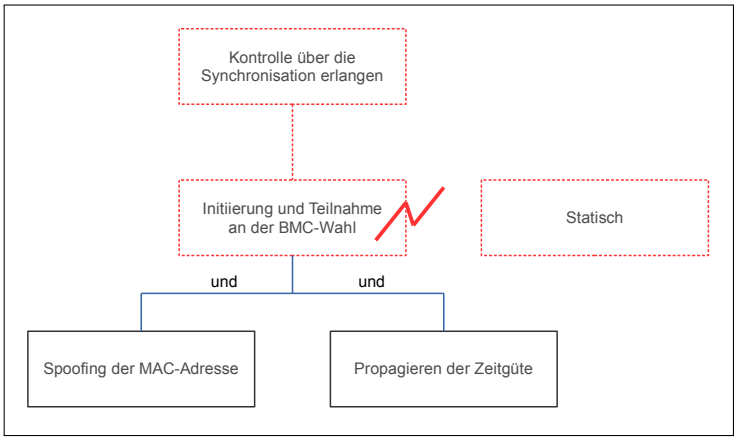

Abbildung 7: Bedrohungsbaum Fallbeispiel Best-Master-Clock-Algorithmus statisch

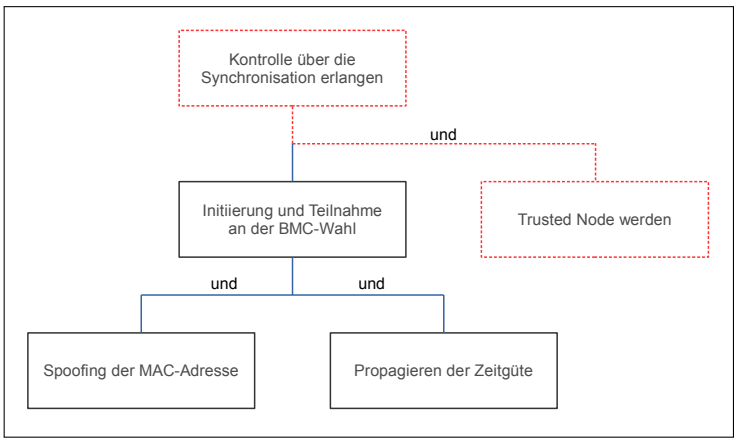

Abbildung 8: Bedrohungsbaum Fallbeispiel Best-Master-Clock-Algorithmus Trusted Node