Informationssicherheit in IEEE 802.1 Time Sensitive Networking Bordnetzen

Philipp Meyer

Wintersemester 2014/15

Zukünftige Fahrzeugbordnetze werden mit Ethernet-Technologien betrieben. Protokolle für eine funktionssichere Echtzeitkommunikation über dieses Medium werden benötigt. Ein vielversprechender Kandidat wird momentan in der IEEE „Time Sensitive Networking Task Group“ standardisiert. Aber wie sieht es mit der Informationssicherheit in so einem Bordnetz aus und welche Mittel stehen zur Entwicklung eines Sicherheitskonzepts zur Verfügung?

1 Einführung

In modernen Fahrzeugen werden mittlerweile eine Vielzahl an Sensoren und Steuergeräten(ECUs) eingesetzt um Technologien zu ermöglichen, die die Funktionssicherheit, die Leistung und den Komfort von Fahrzeugen zu verbessern. Daraus ergeben sich heutzutage immer komplexere Kommunikationsstrukturen, aus verschiedenen proprietären Bustechnologien, und erhöhte Datenmengen. In Zukunft kann durch den Einsatz von Ethernet die Kommunikation dieser Teilnehmer überschaubarer und leistungsfähiger gestaltet werden. Die Echtzeit Anforderungen in diesem Kontext werden mit Protokollen ermöglicht, die auf das Standard Ethernet IEEE 802.3 aufsetzen und damit deren Funktionalitäten und Zuverlässigkeit erweitern. Ein vielversprechender Kandidat ist das Time Sensitive Networking Protokoll. Dieses befindet sich derzeit im Standardisierungsprozess des IEEE([8]). Der Fokus liegt hier aber vor allem auf einer Funktionssicheren Umsetzung. Gegenwärtige Infrastrukturen eines Bordnetzes sind allerdings angreifbar (vgl. [18] und [5]) und führen zu Manipulationen des Fahrzeugverhaltens die mitunter gefährliche Konsequenzen für Fahrzeug und Mensch haben können. Es ist also ein wichtiges Ziel bei der Entwicklung des Fahrzeug-„Nervensystems“ der nächsten Generation von Anfang an adäquate Sicherheitslösungen bereit zu stellen.

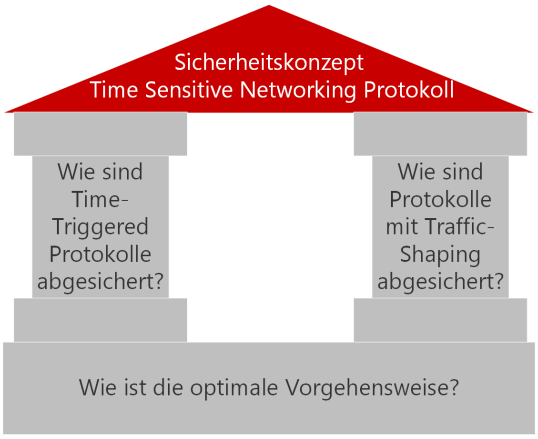

Abbildung 1: Zielsetzung und Aufbau der Arbeit

In dieser Arbeit werden aktuelle Vorgehensweisen zur Entwicklung von Sicherheitskonzepten vorgestellt und in den Kontext von Bordnetzen gesetzt werden. Des weiteren soll ein Überblick des momentanen Forschungsstands im Bereich der Informationssicherheit von Times Sensitive Networking Bordnetzen gegeben werden. Die Abbildung 1 zeigt die Zielsetzung dieser Arbeit im Kontext der Masterarbeit. Die Grauen Bausteine sind Teil dieser Arbeit in deren Verlauf zukünftige Tätigkeiten erarbeitet werden die zu einem Sicherheitskonzept für das Time Sensitive Networking Protokoll führen.

In Kapitel 2 wird de Themenbereich abgegrenzt und die grundlegenden Begriffe erklärt. Danach werden in Kapitel 3 Vorgehensmodelle vorgestellt welche zur Entwicklung und Analyse eines Sicherheitskonzeptes eingesetzt werden können. Hier soll die Frage „Wie ist die optimale Vorgehensweise?“ geklärt werden. Aufbauend darauf gibt es Arbeiten, die sich mit der Sicherheit im Kontext von Bordnetzen und Echtzeitprotokollen beschäftigen. In Kapitel 4 wird auf den momentanen Stand der Informationssicherheit im Time Sensitive Networking Protokoll eingegangen. Die Fragen „Was sind momentane Konzepte zur Absicherung von Time-Triggered Protokollen?“ und „Was sind momentane Konzepte zur Absicherung von Protokollen mit Traffic-Shaping?“ werden beantwortet. Am Schluss folgt mit Kapitel 5 das Fazit und ein Ausblick auf zukünftige Arbeiten.

2 Abgrenzung

In diesem Kapitel wird der Themenbereich mit Hilfe der drei Schlüsselworte „Informationssicherheit“, „Bordnetze“ und „Time Sensitive Networking“ abgegrenzt. Es werden die Grundlagen der Themenbereiche, welche diese Begriffe beschreiben, vermittelt.

2.1 Informationssicherheit

Bei einem sicheren System lässt sich der Begriff „Sicherheit“ in unterschiedliche Bereiche unterteilen. Zum einen ist das die „Informationssicherheit“(Englisch: security). Dieser beschreibt in dieser Arbeit ein System welches keine unautorisierten Veränderung oder Gewinnung von Informationen zulässt. Im Gegensatz dazu beschreibt „Funktionssicherheit“(Englisch: safety) eines in dem Ist- und Sollzustand übereinstimmen.

Bei einem informationssicheren System wird die Funktionssicherheit vorausgesetzt. Des weiteren gibt es drei Basisanforderungen für Informationssicherheit(vgl. [6]):

- Informationsvertraulichkeit: Geheimhaltung der Datenobjekte. Informationen eines Systems sind nur mit entsprechende Autorisierung lesbar.
- Datenintegrität: Verhindern von unauthorisierten Modifikationen an den Datenobjekten. Aktiver Angriffe, mit dem Ziel das Systemverhalten zu verändern, werden verhindert.
- Systemverfügbarkeit: Kein Performance-Verlust. Angriffe(Beispiel: DDoS) können die Leistungsfähigkeit des Systems nicht beeinflussen.

Der Schutz der Informationen ist durch den Schutz der Datenobjekte gewährleistet. Datenobjekte sind zum Beispiel Dateien, Hauptspeicher, Cache oder Kommunikationsnachrichten. Subjekte haben, nur in Abhängigkeit ihrer Zugriffsrechte, Zugriff auf diese Datenobjekte. Die Sicherheit des Gesamtsystems wird nur erreicht, wenn alle Komponenten berücksichtigt werden. Darum ist eine systematische und strukturierte Vorgehensweise bei der Entwicklung von Sicherheitskonzepten notwendig.

2.2 Bordnetze

Das betrachtete System in dieser Arbeit ist das Bordnetz von Fahrzeugen welches die Kommunikation der einzelnen Steuergeräte untereinander ermöglicht. Momentan wird diese durch verschiedene proprietäre Bustechnologien ermöglicht.

In Zukunft kann dieses Technologie Schritt für Schritt durch IEEE 802.3 Switched-Ethernet Netzwerke ersetzt werden (vgl. [1]). Ein Vorteil von Ethernet ist die höhere Bandbreite, die es erlaubt rohe Datenströme von Kameras und anderen Sensoren zu transportieren. Ein andere, dass es eine sehr verbreitete Technologie ist welche dadurch für den Autohersteller kostengünstiger zu beschaffen und weiterzuentwickeln ist. Des weiteren können in Zukunft auf Ethernet aufsetzende Protokolle wie zum Beispiel das Internet Protokoll eingesetzt werden.

Um die Funktionssicherheit eines solchen verteilten Systems zu gewährleisten müssen sogenannte Echtzeitprotokolle eingesetzt werden. Diese erweitern die Funktionalität von Ethernet und garantieren Obergrenzen für Latenz und Jitter in der Kommunikation. Eines dieser Protokolle ist das Time Sensitive Networking Protokoll.

2.3 Time Sensitive Networking

Momentane Protokollkandidaten für die Ethernet-Kommunikation im Automobil sind zum Beispiel Time-Triggered Ethernet (TTE [22]) oder Audio/Video Bridging (AVB [16]). TTE definiert eine Nachrichtenklasse für statisch konfigurierten, synchronen Paketfluss. Diese eignet sich besonders gut für hoch kritischen Datenverkehr, weil Latenzen von bis zu unter 100 µs garantiert werden können. AVB hingegen legt Nachrichtenklassen fest, welche sich dynamisch konfigurieren lassen und asynchron versendet werden. So wird zum Beispiel in IEEE 802.1Qav[12] die dynamische Reservierung von Bandbreiten und Pfaden festgelegt. Mit dem in IEEE 802.1Qat[13] festgelegtem Algorithmus zum Versenden von Paketen lassen sich maximale Latenzen von 2 ms garantieren.

Die Vorteile dieser beiden Stellvertreter zu kombinieren ist das Ziel der „Time Sensitive Networking Task Group“ des IEEE([8]). Es soll ein Protokoll standardisiert werden welches alle Anforderungen der Bordnetzkommunikation in Fahrzeugen erfüllt. Die beiden stellvertretenden Vorgänger werden in der Kombination bereits in Arbeiten analysiert. In der Arbeit [19] wird auf Basis einer Simulation die Leistungsfähigkeit in Abhängigkeit zu unterschiedlichen Konfigurationen untersucht.

Rumpf et al. [20] konzentrieren sich auf die Software-Umsetzung eines kombinierten Stacks für einen Microkontroller. Die Abbildung 2 zeigt den Aufbau der Komponenten des Time Sensitive Networking(TSN) Protokolls.

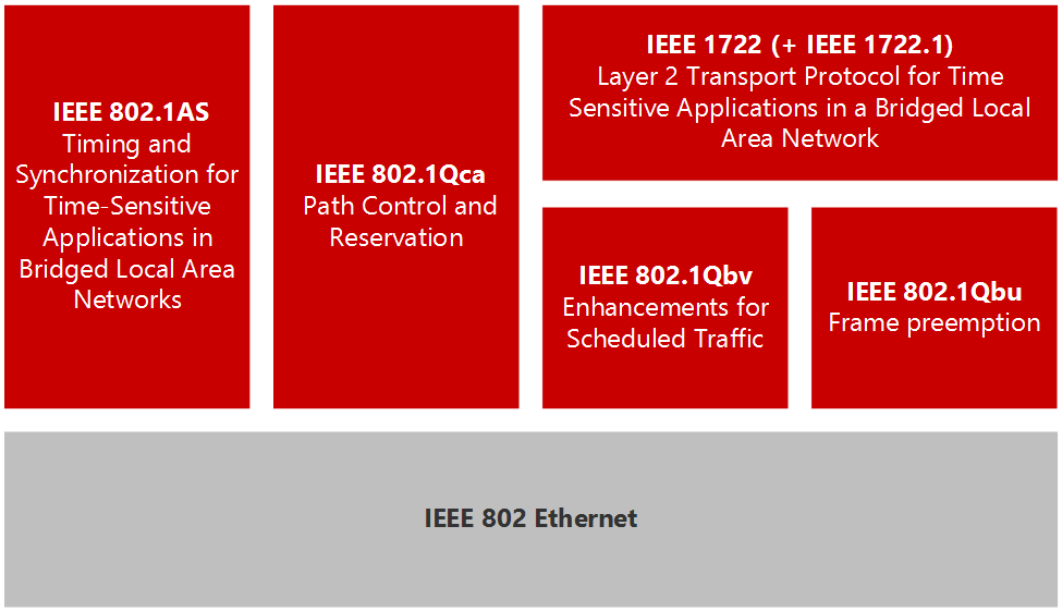

Abbildung 2: Aufbau: Time Sensitive Networking

Die Komponente IEEE 802.1AS[15] ist für die Synchronisation der Zeit zwischen den beteiligten Geräten im Netzwerk zuständig. Mit dieser globalen Zeitbasis steht und fällt der statische Time-Triggered Verkehr des Protokolls da hierfür global eindeutige Zeitpunkte für den Nachrichtentransfer konfiguriert werden müssen. IEEE 802.1Qca[11] beschreibt eine dynamische Seite von TSN. Es kann zur Laufzeit eine benötigte Bandbreite über einen Pfad im Netzwerk reserviert werden. IEEE 802.1Qbv[10] beschreibt das Queueing und Scheduling von Nachrichten am Ausgang eines Netzwerkteilnehmers. Hier könne viele unterschiedliche Algorithmen, zur Weiterleitung von Nachrichten, simultan eingesetzt werden. Beispielsweise ein Kombination aus unpriorisertem Standard Ethernetverkehr, einem klassenabhängigen Trafficshaping (ähnlich: AVB) und einem V-Link abhängigem Time-Triggered Scheduling (ähnlich: TTE). IEEE 802.1Qbu[9] ermöglicht das unterbrechen von Nachrichten. So kann eine hoch priorisierte Nachricht eine niedere auch dann verdrängen wenn diese eigentlich schon auf der Leitung liegt. Je nach Strategie kann der Rest dieser Nachricht dann hinterher gesendet werden. IEEE 1722[14] ist das Transportprotokoll für aufsetzende Anwendungen.

3 Vorgehensmodelle

Eine systematische Vorgehensweise ist das Fundament für die Entwicklung eines Sicherheitskonzepts. Darum werden in diesem Kapitel Vorgehensweisen, die zur Entwicklung von Sicherheitskonzepten dienen, vorgestellt und im Kontext gegenübergestellt. Um die Informationssicherheit in TSN Bordnetzen zu verbessern werden zum einen Grundlagen der IT-Sicherheit herangezogen (siehe [4] und [17]). Zum anderen entwickeln Henniger et al.([7]) Anforderungen an ein Bordnetz für Fahrzeuge. Hier wird ein Prozess zur Identifizierung dieser Anforderungen vorgestellt.

3.1 IT-Grundschutz-Kataloge[4]

Die IT-Grundschutz-Kataloge geben Empfehlungen um Informationen einer Institution zu schützen. Dabei werden, außer technischen, auch organisatorische, personelle und infrastrukturelle Sicherheitsmaßnahmen vorgeschlagen. Die Aufbau ist an das Baukastenprinzip angelehnt. Die Bausteine bilden dabei unterschiedliche Bereiche ab. Innerhalb diese Bausteine wurden ist die Risikoanalyse bereits abgeschlossen. Für einen Grundschutz reicht es dann aus den eigenen Ist-Zustand mit dem Sollzustand des Bausteins zu vergleichen. Bei höheren Anforderungen an die Sicherheit oder Spezialfällen kann die Vorgehensweise zur Risikoanalyse im BSI-Standard 100-3[3] angewendet werden. Die allgemeine IT-Grundschutz Vorgehensweise wird durch den BSI-Standard 100-2[2] beschrieben.

ISO 27001[17] beschreibt ähnliche Schutzempfehlungen. Die Risikoanalyse ist hier aber fester Bestandteil des Vorgehens. Ein Institution kann sich auch mit dem Grundschutz des BSI ISO 27001 Zertifizieren lassen. Der Grundschutzkatalog ist darauf angepasst und bei Unterschieden wird meist ein noch genauerer Rahmen gelegt.

Abbildung 3: Vorgehensweise nach BSI-Standard 100-2[2]

Die Abbildung 3 zeigt die Vorgehensweise nach dem BSI-Standard 100-2. Im ersten Schritt wird der Ist-Zustand analysiert. Danach wird festgestellt für welche Bereich ein Schutzbedarf existiert. Im Dritten Schritt werden die zum Schutzbedarf passenden Maßnahmen aus dem Grundschutzkatalog ausgewählt und über einen Soll-Ist-Vergleich sichergestellt das diese zusammen passen. Darauf hin wird Analysiert ob es noch Schutzbedarf gibt, der bis jetzt nicht befriedigt wurde. Bei ca. 20% der Bereiche ist dieser nicht oder nicht ausreichend der Fall. Hier wird nun eine ergänzende

Risikoanalyse nach BSI Standard 100-3 durchgeführt. In jedem Fall werden dann alle Maßnahmen zusammen getragen. Danach folgt ein zweiter Sicherheitscheck. Als letztes müssen dann die Maßnahmen realisiert werden. Durch ständige Wiederholung kann so ein dauerhafter Grundschutz der Informationen einer Institution gewährleistet werden.

Abbildung 4: Risikoanalyse nach BSI-Standard 100-3[3]

Die Risikoanalyse selber ist in 5 Schritte unterteilt. Diese sind in der Abbildung 4 zu sehen. Als erstes wird ein Übersicht über die Gefährdungen aus erstellt die sich aus dem Grundschutzkatalog entnehmen lassen. Im zweiten Schritt müssen Gefährdungen entdeckt und betrachtet werden welche über das Grundschutz-Modell hinaus gehen. Dabei sollten nur solche aufgenommen werden, die realistisch sind und einen nennenswerten Schaden anrichten können. Im nächsten Schritt wird die Übersicht der Gefährdung abgearbeitet und zu jedem Punkt überprüft ob diese schon ausreichend durch die bisherigen Maßnahmen geschützt sind oder ob es noch keinen Schutz gibt. Nun könne die verbleibenden Risiken behandelt werden. Die kann auf unterschiedliche weise geschehen. Eine Möglichkeit ist den Schutz zu erweitert um die Risiken zu beseitigen. Wenn weiter Schutzmaßnahmen hinzugefügt werden, müssen diese im letzten Schritt mit denn anderen zusammengeführt werden.

Die BSI-Grundschutz-Kataloge bieten eine Rahmen für ein weites Feld an Schutzbedarf. Im Kontext von eines Echtzeit-Ethernet-Protokolls wie TSN ist vor allem die Risikoanalyse nach BSI-Standard 100-3 interessant. Des weiteren ist der Blick über den Tellerrand, durch das Einbeziehen von organisatorischen, personellen und infrastrukturellen Sicherheitsmaßnahmen, ein Punkt der für die Entwicklung eines Sicherheitskonzepts für TSN Beachtung finden muss.

3.2 Sicherheitsanforderungen für Fahrzeugbordnetze[7]

Das beobachtete System von Henniger er al. ist ein Fahrzeug mit unterschiedlichsten ECUs und Schnittstellen. Diese sind über ein heterogenes Bussystem aus CAN- und FlexRay-Bussen miteinander verbunden. Die ECUs sind für alle dinge von Motorsteuerung bis hin zu Infotainment verantwortlich. Die Schnittstellen sind zum Beispiel USB, Bluetooth, GPS und UMTS.

Auf dieser Basis wird ein Prozess vorgestellt der die Entwicklung von Sicherheitsanforderungen eines Bordnetzes ermöglicht. Dieser Prozess besteht aus drei Schritten. Diese sind in der Abbildung 5 festgehalten.

Als erstes werden Bedrohungen identifiziert. Um dies zu erreichen werden Bedrohungsbäume eingesetzt. Dabei ist die Wurzel das Ziel eines Angriffs und Blätter repräsentieren Subziele die das übergeordnete Ziel möglich machen können. Mit logischen Operatoren werden „UND“ und „ODER“ zusammenhänge festgehalten. Die Abbildung 6 zeigt den Aufbau beispielhaft. Auch die Subziele können wiederum Subziele haben. Alle diese Ziele für Angreifer sind Bedrohungen für das System.

Im zweiten Schritt werden die Sicherheitsanforderungen identifiziert, welche die entdeckten Bedrohungen bekämpfen. Hier werden zum einen Anforderungen für die Sicherheit an den System-

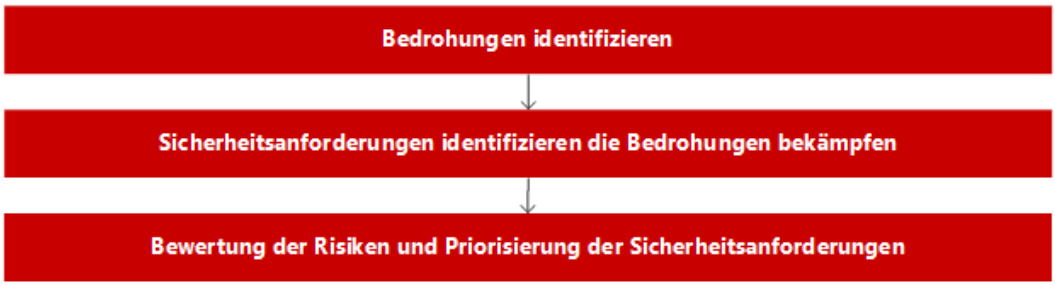

Abbildung 5: Vorgehensweise nach Henniger et al.[7]

grenzen erarbeitet. Diese Systemgrenzen beschreiben hier die Kommunikation von Fahrzeugen untereinander. Zusammen mit den Anforderungen für die detaillierte Funktionalität der Onboard-Systeme(Sensoren, Steuergeräte) wird die Liste der Sicherheitsanforderungen vervollständigt.

Um die wichtigsten Sicherheitsanforderungen zu erkennen werden diese im letzten Schritt priorisiert. Dazu werden die Bedrohungen mit Eintrittswahrscheinlichkeit, Kontrollierbarkeit und Schärfegrad klassifiziert. Der Schärfegrad wird mehrdimensional beschrieben. Auf diese weise kann menschlicher und finanzieller Schaden eingeordnet werden ohne diese gegeneinander gewichten zu müssen. Aus diesen drei Faktoren wird das Risiko berechnet. Auf Basis dessen dann die dazugehörigen Sicherheitsanforderungen priorisiert werden.

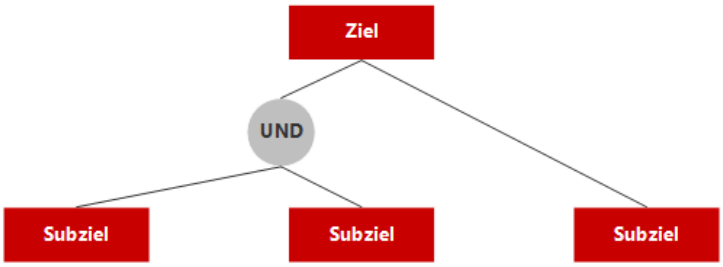

Abbildung 6: Beispiel eines Bedrohungsbaums nach Henniger et al.[7]

Die Vorgehensweise von Hennniger et al. beschreibt im Gegensatz zum BSI-Grundschutz nur die technische Risikoanalyse eines Systems. Die einzelnen Schritte sind enger zusammengefasst und könnten auch feingliedriger beschrieben werden. Der Weg und die eingesetzten Mittel lassen sind gute Kandidaten um für die Entwicklung eins TSN Sicherheitskonzepts einsetzt zu werden. Es zeigt am Beispiel wie die Techniken der IT-Sicherheit im Kontext von Fahrzeugen eingesetzt werden können.

4 Informationssicherheit im Time Sensitive Networking Protokoll

Für „Time-Triggered Ethernet“, den Stellvertreter für synchronen Echtzeitverkehr, gibt es Arbeiten die sich mit deren Informationssicherheit auseinandersetzen. Skopik et al. [21] geben einen Überblick über ein sicheres TTE-System und beziehen sich dabei häufig auf spezifische Funktionalitäten des Protokolls, die viele Bedrohungen implizit verhindern. [23] beschreibt eine Möglichkeit durch Authentifizierung „Time-Triggered“ Übertragungskanäle zu sichern. In diesem Kapitel wird der Aktuelle stand der Forschung von Informationssicherheit in Time Sensitive Networking vorgestellt.

4.1 Sicherheit im Time-Triggered Verkehr

Ein Bestandteil von TSN ist die Möglichkeit Time-Triggered Verkehr zu versenden. Dieser eignet sich perfekt für den Transfer von kritischen Daten. Sie haben Echtzeitanforderungen und müssen garantiert ihr Ziel erreichen. Dafür ist eine gesamten Netz synchronisierte Zeit notwendig. So können Pakete zu global festgelegten Zeitpunkten versendet und empfangen werden.

Die Funktionssicherheit von Time-Triggered Protokollen ist in der Breite abgedeckt und nachweisbar. Im Bereich der Informationssicherheit ist die Forschung aber aktuell.

Skopik er al.[21] geben einen Überblick über ein Informationsicheres Time-Triggered(TT) System. Es wird eine Sicherheitsarchitektur vorgestellt, die auf ein existierendes TT System aufsetzt und sich eng in die Mechanismen für die Funktionssicherheit integriert.

Die Hauptbestandteile der Architektur sind Geräteauthentifizierung, sichere Uhrensynchronisation und die Sicherung der Anwendungsschicht.

Die Geräteauthentifizierung stellt die Datenintegrität her. So müssen sich Geräte gegenseitig Authentifizieren wenn sie miteinander Kommunizieren wollen. Auf diese weise kann verhindert werden, dass infizierte Geräte hinzukommen oder „man-in-the-middle“ Angriffe zum Erfolg führen. Dabei müssen diese Mechanismen die Eigenschaften des TT Verkehrs beachten. Ein unvorhergesehenes Delay durch den Authentifizierungsmechanismus muss verhindert werden.

Die sichere Uhrensynchronisation ist ein wesentlicher Bestandteil. Wenn ein Angreifer die Uhren der Netzteilnehmer auseinander driften lässt bricht das komplette System auseinander. Im Falle von „Time-Triggered Ethernet“ ist diese zumindest Fehlertolerant. Um die Synchronisation auch gegen Angriffe zu schützen wird das Protokoll um Sicherheitsfeatures erweitert. Die Synchronisationsnachrichten bekommen eine Signatur und Messungen müssen durchgeführt werden um falsche Zeitangaben zu erkennen.

Die Anwendungsschicht kann dann darauf Aufsetzend Informationsvertraulichkeit und Datenintegrität hinzufügen. Auf diese weise sind die Informationen geschützt selbst wenn der Angreifer physikalischen Zugriff auf das Netz hat. Dabei kann die sicher synchronisierte Uhr als Basis für leistungssparende Algorithmen eingesetzt werden.

Insgesamt wird ein Konzept vorgestellt, dass mit minimierten Mehraufwand die Informationssicherheit von reinen TT Protokollen umsetzen kann. Nähere technische Details werden allerdings nicht erläutert. Dies ist vor allem dem Umstand geschuldet, dass eine konkrete Umsetzung noch nicht durchgeführt ist.

In der Arbeit von Wasicek et al.[23] wird eine konkrete Umsetzung für Authentifizierung in TT Systemen vorgestellt.

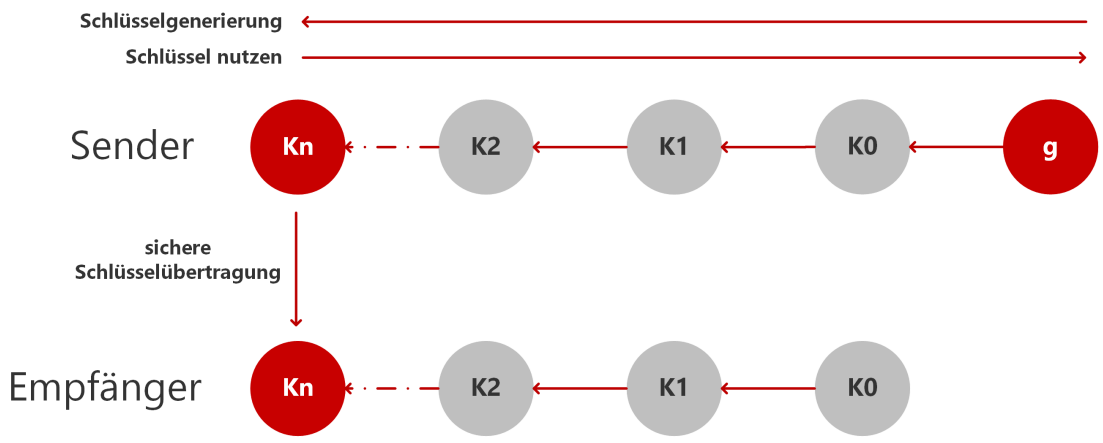

Abbildung 7: KeyChain nach Wasicek et al.[23]

Die TT Synchronisationspakete werden dabei mit einem Schlüssel signiert. Der jeweilige Schlüssel ist dabei Teil einer Schlüsselkette. Die Abbildung 7 zeigt die Funktionsweise von diesem Mechanismus.

Nur der Sender muss einen Schlüssel K0 aus g generieren. Danach wird die Schlüsselkette erstellt. Mit einer Hashfunktion wird aus K0 K1 erzeugt aus K1 K2 bis schließlich Kn erzeugt ist und die Schlüsselkette damit abgeschlossen ist. Mit den Schlüssel werden nun die TT Nachrichten rückwärts signiert.

Nur beim ersten mal, mit dem Schlüssel Kn, geschieht dieses über einen, durch ein asymmetrisches Verfahren, gesicherten Übertragungsweg. So kennen nur die Empfänger den Schlüssel Kn. Nun können die Empfänger mit jeder eingehenden Nachricht die sie empfangen die vorangegangene Authentifizieren. Er kann nun durch anwenden der gleichen Hashfunktion den Schlüssel der vorangegangen Nachricht erzeugen und muss diese dann abgleichen. Auch wenn ein Glied in der Kette fehlt kann durch zweimaliges Anwenden der Hashfunktion der Vorgänger authentifiziert werden.

Wenn die Schlüsselkette aufgebraucht ist generiert der Sender eine neue.

Mit dieser Technik wird der Rechenaufwand der Netzteilnehmer für die sichere Kommunikation reduziert. Der Sender muss allerdings Speicher für die Schlüsselkette zur Verfügung stellen. So ergibt sich ein Tradeoff verhalten zwischen der Häufigkeit der Schlüsselgenerierung und dem Speicherverbrauch.

Wasicek er al. zeigen eine effiziente Möglichkeit zur Authentifizierung von Netzwerkteilnehmern in einem Time-Triggered System. Mechanismen in dieser Art sind im Kontext von Fahrzeugbordnetzen wichtig, da die Leistungsfähigkeit der Hardware stark begrenzt ist.

4.2 Sicherheit im Traffic-Shaping Verkehr

Im Bereich von Traffic-Shaping Verkehr und dem TSN Vorgänger Audio-/Video Bridging(AVB) gibt es noch keine aktuellen Forschungsarbeiten. So ist es notwendig in Zukunft einen verstärkten Fokus auf dieses Problem zu setzen um die Schwachstellen zu ergründen. Dies muss strukturiert mit den vorgestellten Mitteln aus Kapitel 3 durchgesetzt werden. Die zukünftigen Entwicklungen in diesem Bereich müssen dabei weiterhin beobachtet werden. Des weiteren kann suche noch breiter durchgeführt werden um vielleicht andere für den Kontext relevante Arbeiten zu finden.

5 Fazit und Ausblick

Vorgehensweisen zur Entwicklung von Sicherheitskonzepten sind etabliert. Diese sind vor allem in den IT-Grundschutz-Katalogen festgehalten. Henniger et al. zeigen eine Übertragung des Werkzeugkastens IT-Sicherheit in den Kontext von Fahrzeugen.

Der aktuelle Stand der Forschung im Bereich der Informationssicherheit in Time Sensitive Networking Bordnetzen ist unterschiedlich ausgeprägt. So gibt es einige Ansätze zum Schutz von Time-Triggerd Verkehr. Skopik er al. stellen ein gesamt Konzept für ein TT System vor mit dem die Informationssicherheit in einem solchen Netz gewährleistet werden kann. Wasicek et al. zeigen einen konkreten Lösungsansatz für die Authentifizierung von Netzwerkteilnehmern. Dieser ist Ressourcensparend und passt so zu den Anforderungen eines Bordnetzes. Im Bereich von Traffic-Shaping Verkehr, welcher eine andere Ausprägung von TSN beschreibt, ist die Frage nach Informationssicherheit bis offen. So gibt es bis heute keine Arbeiten die den Schutzbedarf festgestellt haben oder Ansätze zum Schutz des Verkehrs liefern.

Für das weitere Vorgehen gibt es drei identifizerte Basisrisiken. Das erste ist die Vollständigkeit. Es besteht die Gefahr, dass Lücken im Protokoll übersehen werden und die Informationssicherheit dadurch gefärdet ist. Der zweite Punkt ist die Umsetzbarkeit. Ist das Sicherheitskonzept am Ende auch praktisch anwendbar? Es kann sein, dass die Lösung durch Ressourcenverbrauch oder ähnliches in der Paxis nicht einsetzbar ist. Das letzte Risiko ist die Erfahrung. Durch mangelnde Erfahrung kann der Entwicklungsprozess in die länge gezogen werden. Weitere Risiken können im weiteren Verlauf mit den nächsten Arbeiten entstehen.

Diese nächsten Schritte zu einem Sicherheitskonzept für TSN sind nun notwendig:

Als erstes muss in Projekt 1 eine konkrete Vorgehensweise erarbeitet werden, welche über den weiteren Verlauf fest eingehalten wird um Vollständigkeit im Sicherheitskonzept zu erreichen. Dann muss eine Analyse stattfinden um die Schwachstellen auf zu decken. Diese wird sich vor allem auf den Bereich dese Traffic-Shaping Verkehrs fokussieren. Methoden zu schließen der Schwachstellen müssen aufgedeckt und entwickelt werden.

In Projekt 2 soll dann eine Prototypentwicklung stattfinden. Anhand dessen Schutzkonzepte evaluiert werden können. Es muss die frage geklärt werden ob dieser in Simulation oder echter Hardware realisiert wird.

In der anschließenden Masterarbeit wird dann Schutzmethoden ein Sicherheitskonzept konsolidiert. Dieses soll die Informationssicherheit in, mit TSN betriebenen, Bordnetzen gewährleisten. Das wird darauf hin mit dem Prototypen evaluiert. So das am Ende ein evaluiertes Sicherheitskonzept für TSN im Bordnetzeinsatz von Fahrzeugen zur Verfügung steht.

Literatur

[1] Bruenglinghaus, C. ; Redaktion Springer fuer Professionals: *Am Ethernet im Auto fuehrt kein Weg vorbei.* http://www.springerprofessional.de/am-ethernet-im-auto-fuehrt-kein-weg-vorbei/4979586.html

[2] Bundesamt fuer Sicherheit in der Informationstechnik: *BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise.* https://www.bsi.bund.de/DE/Publikationen/BSI_Standard/it_grundschutzstandards.html

[3] Bundesamt fuer Sicherheit in der Informationstechnik: *BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz.* https://www.bsi.bund.de/DE/Publikationen/BSI_Standard/it_grundschutzstandards.html

[4] Bundesamt fuer Sicherheit in der Informationstechnik: *IT-Grundschutz-Kataloge.* www.bsi.de/gshb

[5] Checkoway, S. ; Mccoy, D. ; Kantor, B. ; Anderson, D. ; Shacham, H. ; Savage, S. ; Koscher, K. ; Czeskis, A. ; Roesner, F. ; Kohno, T. : Comprehensive Experimental Analyses of Automotive Attack Surfaces. In: *USENIX Security* (2011). http://static.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf

[6] Eckert, C. : *IT-Sicherheit Konzepte - Verfahren - Protokolle.* 8., aktualisierte und korr. Aufl. Muenchen : Oldenbourg, 2013

[7] Henniger, O. ; Apvrille, L. ; Fuchs, A. ; Roudier, Y. ; Ruddle, A. ; Weyl, B. ; Paristech, T. ; Ltci, C. ; Antipolis, S. : Security requirements for automotive on-board networks. (2009), S. 641–646. ISBN 9781424453474

[8] IEEE 802.1 TSN Task Group: *IEEE 802.1 Time-Sensitive Networking Task Group.* http://www.ieee802.org/1/pages/tsn.html

[9] IEEE 802.1 TSN Task Group: *IEEE 802.1Qbu - Frame Preemption.* http://www.ieee802.org/1/pages/802.1bu.html

[10] IEEE 802.1 TSN Task Group: *IEEE 802.1Qbv - Enhancements for Scheduled Traffic.* http://www.ieee802.org/1/pages/802.1bv.html

[11] IEEE 802.1 TSN Task Group: *IEEE 802.1Qca - Path Control and Reservation.* http://www.ieee802.org/1/pages/802.1ca.html

[12] Institute of Electrical and Electronics Engineers: IEEE 802.1Qav - IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks - Amendment 12: Forwarding and Queuing Enhancements for Time-Sensitive Streams / IEEE. 2009 (IEEE 802.1Qav-2009). – Standard. – ISBN 978–0–7381–6143–3

[13] Institute of Electrical and Electronics Engineers: IEEE 802.1Qat - IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks - Amendment 14: Stream Reservation Protocol (SRP) / IEEE. 2010 (IEEE 802.1Qat-2010). – Standard. – ISBN 978–0–7381–6501–1

[14] Institute of Electrical and Electronics Engineers: IEEE 1722 - IEEE Standard for Layer 2 Transport Protocol for Time Sensitive Applications in a Bridged Local Area Network / IEEE. 2011 (IEEE 1722-2011). – Standard. – ISBN 978–0–7381–6549–3

[15] Institute of Electrical and Electronics Engineers: IEEE 802.1AS - IEEE Standard for Local and metropolitan area networks - Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks / IEEE. 2011 (IEEE 802.1AS-2011). – Standard. – ISBN 978–0–7381–6536–3

[16] Institute of Electrical and Electronics Engineers: IEEE 802.1BA - IEEE Standard for Local and metropolitan area networks - Audio Video Bridging (AVB) Systems / IEEE. 2011 (IEEE 802.1BA-2011). – Standard. – ISBN 987–0–7381–7639–8

[17] *Information technology – Security techniques – Information security management systems – Requirements.* 2013

[18] 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: *2010 IEEE Symposium on Security and Privacy (SP)*, 2010. – ISSN 1081–6011, S. 447–462

[19] Meyer, P. ; Steinbach, T. ; Korf, F. ; Schmidt, T. : Extending IEEE 802.1 AVB with time-triggered scheduling: A simulation study of the coexistence of synchronous and asynchronous traffic. In: *Vehicular Networking Conference (VNC), 2013 IEEE*, 2013, S. 47–54

[20] Rumpf, S. ; Steinbach, T. ; Korf, F. ; Schmidt, T. C.: Software Stacks for Mixed-critical Applications: Consolidating IEEE 802.1 AVB and Time-triggered Ethernet in Next-generation Automotive Electronics. In: *2014 IEEE International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*. Piscataway, New Jersey : IEEE Press, 2014. – ISBN 978–1–4799–6165–8, S. 14–18

[21] Skopik, F. ; Treytl, A. ; Geven, A. ; Hirschler, B. : Towards secure time-triggered systems. In: *..., Reliability, and Security* (2012), 1–8. http://link.springer.com/chapter/10.1007/978-3-642-33675-1_33

[22] Society of Automotive Engineers - AS-2D Time Triggered Systems and Architecture Committee: *Time-Triggered Ethernet AS6802.* SAE Aerospace. http://standards.sae.org/as6802/. Version: Nov. 2011

[23] Wasicek, A. ; El-Salloum, C. ; Kopetz, H. : Authentication in Time-Triggered Systems Using Time-Delayed Release of Keys. In: *2011 14th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing* (2011), März, 31–39. http://dx.doi.org/10.1109/ISORC.2011.14. – DOI 10.1109/ISORC.2011.14. ISBN 978–1–61284–433–6