h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

Exposé

zu meiner Bachelorarbeit

„Verschlüsselung des Controller Area Network mit kryptografischen Mitteln“

Jannis Priesnitz

Referent: Prof. Moore

Coreferent: Prof. Wiedling

27. April 2015

1 Problemstellung

Das Controller Area Network (CAN) wird in einer Vielzahl von Systemen, vor allem im Bereich eingebetteter Systeme, eingesetzt. Eine Vielzahl davon enthalten sicherheitskritische Komponenten, deren Ausfall weitreichende Konsequenzen nach sich ziehen sowie Risiken für den Anwender darstellen. Beispiele hierfür sind der Ausfall des Antiblockiersystems während der Autofahrt oder das Einschleusen von Schadsoftware in Kraftwerken oder Fabriken. Nach aktuellem Stand der Technik wird das Controller Area Network komplett ohne eine Verschlüsselung der übertragenen Informationen und Authentifikation der Teilnehmer verwendet. Die Sicherheit beruht derzeit ausschließlich auf der Abgeschlossenheit des Systems sowie des meist geheimgehaltenen Softwareprotokolls.

Vor allem moderne Autos bieten jedoch die Möglichkeit durch „Basteleien“ Busteilnehmer auszutauschen und so Schadsoftware in das System gelangen zu lassen.

Des weiteren können Komponenten, die andere Schnittstellen wie z.B. W-Lan besitzen, übernommen werden und so über das CAN[1] sicherheitskritische Komponenten infizieren.

2 Erkenntnisinteresse

Um die Sicherheit von technischen Anlagen und Automobilen, die CAN nutzen, zu gewährleisten, muss darüber nachgedacht werden, wie dies auf einem akzeptablen Niveau geleistet werden kann. Die Idee einer Verschlüsselung wurde bereits durch verschiedene Firmen betrachtet und soll hier aufgenommen und um den Aspekt der Instanzauthentifikation ergänzt werden. Dies ist speziell für Systeme, in denen Komponenten einfach von unautorisierten Menschen ausgetauscht werden können, wie z.B. im Auto, von großer Bedeutung.

Das zu erstellende Konzept zeigt den Aufwand für solch ein Vorhaben auf und gibt eine Einschätzung über deren Machbarkeit. Hierzu werden sowohl gängige kryptografische Mittel von mir ausgewählt, um maximale Sicherheit zu gewähr-

[1] Da es sich bei CAN um die Abkürzung für Controller Area Network handelt, wird CAN im Folgenden so verwendet.

leisten, als auch Messungen an einer exemplarisch ausgewählten Untermenge mit geringerem Sicherheitsniveau (einem Subset an Sicherheit) von mir durchgeführt.

Meine Aufgabe besteht zusammenfassend darin, die bereits gewonnen Erkenntnisse aus dem Bereich der Kryptografie und der Embedded Systems zusammen zu bringen und ein fundiertes Konzept über die Möglichkeiten zu geben.

3 Fragestellung

Zentrale Fragestellung der Arbeit ist es, ob es effizient möglich ist, *eine* verschlüsselte und authentische Kommunikation in dem CAN durchzuführen.
Dies unterteilt sich zunächst prinzipiell in den Aufwand für die Initialisierung der Kommunikation und den zusätzlichen Aufwand für verschlüsselte Kommunikation zur Laufzeit.
Weiter soll die Frage geklärt werden, *welche Mittel* eingesetzt werden müssen, um ein maximales Sicherheitsniveau nach dem Stand der Technik zu erreichen. Hieraus resultiert direkt die Aufgabe, geeignete kryptografische Mittel für die gegebenen Hardwarevoraussetzungen auszuwählen und eine Abschätzung der Performance zu geben.
Die theoretischen Betrachtungen sollen anhand der Frage, *wie performant* ein von mir gewähltes und prototypisch implementiertes Subset an Sicherheit sein kann, untermauert werden.
Die Eigenschaften und Vorzüge des Netzwerkes müssen hierbei soweit, wie möglich gewahrt bleiben und Einschränkungen hinsichtlich der Kommunikationsteilnehmern sollen genau beschrieben und begründet werden. Ferner wird kurz auf die Hardwarevoraussetzungen eingegangen, die ein Kommunikationsteilnehmer mitbringen sollte, um die gewählten Algorithmen durchführen zu können.

4 Zielsetzung

Es soll gezeigt werden, dass eine verschlüsselte und authentische Kommunikation nach dem Stand der Technik über das CAN grundsätzlich möglich ist. Darüber hinaus soll auf die besonderen Randbedingungen bei einem Einsatz im automoti-

ve embedded Umfeld eingegangen werden. Außerdem sollen gängige kryptografische Mittel ausgewählt werden, um dies zu realisieren und deren Wahl kurz begründet werden. An einer prototypischen Implementierung einer Teilmenge sollen Messwerte genommen werden, anhand derer eine differenzierte Aussage über die Realisierbarkeit einer sicheren Kommunikation getroffen werden kann. Aus diesen Ergebnissen wird anhand von Komplexitätsabschätzungen auf die Realisierbarkeit und Performance der maximalen Sicherheit geschlossen.

5 Theoriebezug und Modellbildung

Die Arbeit basiert auf der Theorie, dass jede Kommunikation durch geeignete Mittel verschlüsselt und authentisch statt finden kann, welche letztendlich auf der mathematischen Gruppentheorie basiert. Es wird ein Modell gebildet, welches die Kommunikation zwischen mehreren Kommunikationspartnern betrachtet und in ähnlicher Weise (in Bezug auf Chipperformance) in aktuellen Systemen, die das CAN-Protokoll nutzen, zum Einsatz kommen könnte. Das Modell ist hinsichtlich Kommunikationsteilnehmern und kryptografischer Sicherheit gegenüber der Realität eingeschränkt. Es soll ein Multiproducer - Multiconsumer Modell betrachtet werden, in dem die Kommunikation von einem zentralen Server geregelt wird. Dieser Server verwaltet eine oder mehrere Domains, deren zwei oder mehr Clients angehören.

6 Methode

Es wird ein Prototyp erstellt, der ein Subset einer sicheren Kommunikation darstellt. Anhand dieser Implementierung werden verschiedene Algorithmen mit unterschiedlichen Randbedingungen getestet. Aus den Ergebnissen werden Empfehlungen für alternative Algorithmen und Verfahren und eine Abschätzung der Effizienz dieser gegeben.

7 Vorläufige Gliederung

Nach aktuellem Erkenntnissen gestaltet sich eine Gliederung folgendermaßen:

1. Einleitung / Hintergrund
2. Aufgabenstellung
    - Authentische Kommunikation
    - Verschlüsselte Kommunikation
3. Randbedingungen der Automotive Embedded Welt und von CAN
    - Rechenleistung
    - Speicherverwaltung
    - Betrachtungen zu Multithreadingeigenschaften
    - Ausfallsicherheit
4. Konkretes Design der prototypischen Implementierung
    - Authentisierung
    - Schlüsseltausch
    - Verschlüsselung
5. Performancemessungen
    - Setup Zeit
    - Lauftzeit einer Nachricht
    - Speicher
6. Kryptografisches System mit maximaler Sicherheit
    - Vorstellung des Systems
    - Abschätzung der Realisierbarkeit aufgrund der Messungen am Prototyp
7. Fazit und Ausblick

8 Literaturverzeichnis

Die bis jetzt von mir recherchierten, zentralen Quellen sind im Folgenden angegeben. Weitere Quellen sind noch zu beschaffen.

Literatur

[1] *CAN Specification Version 2.0.*

[2] Konrad Etschberger. Controller area network: basics, protocols, chips and applications. 2001.

[3] Armin Happel. Verschlüsselte signalübertragung mit autorsar in einem can-fd-netzwerk. 2014.

[4] NIST FIPS Pub. 197: Advanced encryption standard (aes). *Federal Information Processing Standards Publication*, 197:441–0311, 2001.

[5] John Viega, Matt Messier, and Pravir Chandra. *Network Security with OpenSSL: Cryptography for Secure Communications.* Ö'Reilly Media, Inc.", 2002.

[6] Brigitte Werners and Phillip Klempt. Management von it-risiken in supply chains. *Risikomanagement in Supply Chains–Gefahren abwehren, Chancen nutzen, Erfolg generieren, Berlin*, 2007.

[7] Joachim Wietzke and Manh Tien Tran. *Automotive Embedded Systeme: Effizfientes Framework-Vom Design zur Implementierung.* Springer-Verlag, 2006.

9 Zeitplan

24.04.2015	Anmeldung zu Bachelorarbeit
27. April 2015	Abgabe des Exposès
27. April 2015- 15.05.2015	Fertigstellung des Prototypen (und ende Praxisphase)
15.05.2015 - 07.06.2015	Messungen am Prototyp und Auswertung
07.06.2015 - 14.06.2015	Design eines Systems mit maximaler Soicherheit
15.06.2015 - 29.06.2015	Betrachtungen zu den Verausetzungen für einzusetzende Systeme
29.06.2015 - 17.07.2015	Schlussfolgerung der Performance des Prototype auf das System maximalere Sicherheit
18.07.2015 - 23.07.2015	Korrektur und Verbesserungen
24.07.2015	Abgabe der Bachelorarbeit