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

3. Mai 2015

Inhaltsverzeichnis

1 Einleitung

in meiner Praxispahase...

1.1 Motivation

In meinem Studium hatte ich die Gelegenheit einige Vorlesungen im Bereich der technischen Informatik zu Belegen, die mir durch ihre Nähe zur Hardware und Komplexität besonders gefallen haben.

2 Das Unternehmen

2.1 Überblick

Die Continental Automitive AG ist ein Konzern der Automobilzuliefererbrache mit 190000 Mitarbeitern, an über 200 Standorten und 53 Ländern. Der Hauptsitz befindet sich in Hannover. Neben dem ehemaligen Kerngeschäft, der Reifenproduktion, ist Continental einer der größten Automobilzulieferer weltweit. Zu den Kunden gehören neben allen großen deutschen Automobilherstellern Weltweit viele namhafte Autokonzerne.

2.2 Unternehmensbereiche (Divisionen)

Die Continental Automotive AG unterteilt sich in fünf Divisionen, die ich hier kurz vorstellen möchte.

Chassis & Safety Die Division Chassis and Safety entwickelt Fahrsicherheitssysteme, wie elektronische und hydraulische Bremssysteme, Sensorsysteme, sowie passive Sicherheitssysteme (z.B. Airbags) und Fahrassistenzsysteme (z.B. ABS)

Powertrain Die Division Powertrain beschäftigt sich mit Lösungen rund um den Antriebsstrang von Fahrzeugen. Dazu gehören Komponenten für Motoren, Getriebe und Kraftstoffversorung, sowie mit dem Thema der Elektromobilität.

Tires Die Division Tires ist mit der Entwicklung von Reifen für PKW und LKW befasst.

ContiTech Die Division ContiTech spezialisiert sich auf Kautschuk und Kunststofftechnologie abseits der Reifen und hat zur Aufgabe Federungssysteme, Beförderungssysteme, Antriebsriemen, Membranstoffe, und außerdem Flüssigkeitstechnologien zu entwickeln.

Interior Die Division Interior, der ich während der Praxisphase angehörte, fasst sämtliche Aktivitäten die das Darstellen und Auswerten von Informationen im Fahrzeug zusammen. Dabei steht die Schnittstelle zwischen Mensch und Maschine im Vordergrund. Geschäftsbereiche der Division sind Instrumentation and Driver HMI, in dem er um die optische und grafische Aufbereitung von Informationen geht, Infotainment and Connectivity, in der Infotainmentsystem entwickelt werden, Body and Security, die sich mit Schließsystemen, sowie die Verfügbarkeit der Funktionen im Auto sicherstellt und Commercial Vehicles & Aftermarket die sich um spezifische Anforderungen im Bereich von Nutzfahrzeugen und Vertrieb kümmert.

2.2.1 Bereich Core Development Software

Der Geschäftsbereiche '"Core Development Software (CDS)‘ist die zentrale, technologische Authorität im Geschäftseinheit Instrumentation & Driver HMI. Die zentrale Aufgabe besteht darin, die technologische Führereschaft des Geschäftsbereiches durch hohe Softwarequalität weiter auszuweiten. Dies geschieht durch Entwicklung bereits bestehender und neuer Softwarekompinenten und Plattformen, Forschung an neuen Technologien, Qualitätssicherung und Support beim Kunden. Ziel ist es dem OEM eine einheitliche, sichere, fortschrittliche skalierbare Plattform nach seinen Anforderungen zur Verfügung zu stellen, sodass diese mit einheitlichen Prozessen beim Kunden weiterentwickelt werden kann. Das CDS umfasst die Technologien Grafik, HMI, Sound, Betriebsystem, Netzwerk, Treiber, Diagnose und Flash / Bootloader, der ich angehöre.

2.2.2 CDS Gruppe Flashbootloader

Die Flashbootloader Gruppe beschäftigt sich mit der Entwicklung eines einheitlichen plattform- und technologieunabhägigen Flashprozesses und der Bereitstellung eines einfachen Systems zum Flashen von Systemen und Anwendungen für die Anwendungsentwichlung. Außerdem wird eine End-of-Line Diagnose bereitgestellt, die eine einfache Analyse des abgeschlossenen Fashprozesses zulässt. Weiter werden Software Pakete für Speichertechnologien für andere Teams bereitgestellt.

2.3 Produkte

Wie bereits im Punkt Unternehmensbereich beschrieben, entwickelt und fertigt Continental sehr viele verschiedene Komponenten und ganze Systeme für die Automobilindustrie. Besonders möchte dabei auf die Entwicklung von Kombiinstrumenten, Head-up Displays und ähnlichen informationstechnischen Komponenten eingehen, die von der Business Unit Instrumentation & Driver HMI übernommen wird. Dies geschieht am Standort Babenhausen in Verbindung mit den Standorten Singapur, Timisoara (Rumänien) und ferner Guadalajara (Mexiko) entwickelt und in Babenhausen gefertigt werden.

2.4 Meine Praxisstelle - organisatorische Einbettung

Für diese Komponenten werden in der Abteilung, in der ich tätig bin Flashbootloader entwickelt. Meine Aufgabe hat zunächst nichts mit den primären Aufgaben Abteilung zu tun, in der ich sitze, jedoch ist eine mögliche Schnittstelle über die der Flashvorgang stattfinden kann, das Controller Area Network CAN. Dieser Vorgang, der nicht nur im Werk, sondern auch beim Endkunden in einer Werkstatt stattfinden kann, soll gegen eingriffe von außen abgesichert werden. Hieraus resultiert ein möglicher Anwendungsfall für das von mir zu erstellende Konzept.

3 Das Projekt

CANKrypto blabla

3.1 Allgemeine Beschreibung

Der Titel des von mir bearbeiteten Projektes lautet 'SSichere Kommunikation über das Controller Area Netzwork (CAN)„. Ziel des Projektes ist es geeignete Mittel für ein sichere Kommunikation auszuwählen und den zusätzlichen Aufwand dafür abzustecken. Hierbei ist vor allem für eine Eignung der/des XXX im Umfeld von Embedded Systemen zu achten. Das Projekt wurde Hausintern aufgrund von Kundenanforderungen generiert, der eine Absicherung sämtlicher Plattformen und Schnittstellen wünscht. Die Ergebnisse des Konzeptes werden ggf. später in die Entwicklung neuer Flashprozesse einfließen oder als Sicherung der Kommunikation zwischen Komponenten im Auto eingesetzt werden.

3.2 Meine Aufgabe

Meine Aufgabe ist es ein Konzept für eine sichere Kommunikation über das Controller Area Network (CAN) zu erstellen. Dabei sollen vor allem die Aspekte einer Instanzauthentifikation der Kommunikationsteilner und eine Verschlüsselung der zu übertragenen Nachrichten betrachtet werden.

3.3 Ziele

Ziel meiner Praxisphase und der daraus resultierenden Bachelorarbeit ist es die Machbarkeit der sicheren Kommunikation über das CAN Protokoll zu beurteilen. Dabei wurde mir ein sehr großer Spielraum bei der Aufgabenplanung und der Umsetzung gewährt.

Dazu sollen kryptografische Mittel nach aktuellem Stand der Technik ausgewählt und ein Vorschlag für ein Kommunikationsprotokoll gemacht werden, das eine für die Anwendungsschicht transparente Kommunikation gewährleistet. Die gewählten Ansätze sollen in Software umgesetzt werden und hinsichtlich Performance, Speicherverbrauch und Portabilität geprüft werden.

Eine Betrachtung auf unterschiedlichen Zielsystemen, wie z.B. dem JCP2011 und Betriebssystemen (Linux, Autosar os, QNX) steht noch aus.

3.4 Eingesetzte Technologien

C Visuual Studio CrypoPP, CryptLib, OpenSSL BBB Make mingw Linux

3.5 Anforderungen

3.6 Konzepte und Lösungsansätze

wurden komplett von mir entwickelt

3.7 Aktueller Stand

Prototyp Messungen

3.8 Bewertung des Ergebnisses

- Viel geschafft viel muss noch getan werden

3.9 Ausblick

Auch wenn dies ein Abschlussbericht ist, möchte ich kurz auf meine weiteren Tätigkeiten im Rahmen der noch verbleibenden Zeit in der Praxisphase geben. Außerdem möchte ich noch kurz einen generellen Ausblick zu der von mir bearbeiteten Thematik geben.

4 Evaluation der Praxisphase

4.1 Das Unternehmen

4.2 Lessons Learned

Crypto API schneller wählen+ direkt c entwickeln

4.3 Persöhnliche Einschätzung des Lernerfolgs