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

2. Mai 2015

Inhaltsverzeichnis

1 Einleitung

in meiner Praxispahase...

1.1 Motivation

meine Praxisphase habe ich gemacht bei conti weil..

2 Das Unternehmen

Die Continental Automitive AG entwickelt und baut am Standort Babenhausen Kombiinstrumente, Head-up Displays (HUDs) und ähnliche informationstechnische Komponenten im Bereich von automotive embedded Systems für zahlreiche Automobilhersteller weltweit. Dabei wird nahezu jedes Bauteil und jede Softwarekomponente selbst entwickelt und produziert.

2.1 Mein Tätigkeitsbereich

Meine Praxisphase absolviere ich in der **Devision „Interior“** im **Bereich „Instrumentation & Driver HMI“**, welcher sich mit der Entwicklung von modernen Kombiinstrumenten, Head-up Displays und Steuerungseinheiten im Cockpit eines Autos beschäftigt.

Die Einheit „Core Development Software (CDS)“ entwickelt eine Basis für die Anwendungsentwicklung durch einheitliche Technologien, Standards und Lösungen, die das Durchführen von Softwareprojekt unter einheitlichen Standards und Prozessen und Plattformen unterstützt. Außerdem werden neue Technologien erforscht und bestehende verbessert.

Die Gruppe „Flash/Bootloader“ schließlich entwickelt Flashloader Systeme, die für das aufspielen und das starten des Systems verantwortlich sind, sowie Packaging- und Diagnosesysteme in Verbindung mit Flashspeichern. Ziel ist es einen einheitlichen, einfachen und sicheren Flashprozess sowohl in der Fertigung,

als auch beim Endkunden zu gewährleisten und Fehlfunktionen schnell zu diagnostizieren, sowie eine lange Lebensdauer der Flashspeicherbausteine zu erreichen.

2.2 Produkte

2.3 Unternehmensbereiche

2.4 organisatorische Einbettung

3 Das Projekt

CANKrypto blabla

3.1 Allgemeine Beschreibung

3.2 Meine Aufgabe

Meine Aufgabe ist es ein Konzept für eine **sichere Kommunikation über das Controller Area Network (CAN)** zu erstellen. Dazu soll ein bestehendes CAN-Demoprogramm umfassend umgebaut werden, kryptografische Verfahren und Parameter ausgewählt werden und diese in das CAN-Setup integriert werden. Außerdem soll die Software auf verschiedene Hardwar- und Betriebssystemen integriert und umfassende Performancetests durchgeführt werden.

3.3 Ziele

Ziel des Konzeptes ist es die Machbarkeit der sicheren Kommunikation über das CAN Protokoll zu beurteilen. 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.

3.4 Eingesetzte Technologien

C Visuual Studio CrypoPP, CryptLib, OpenSSL

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