h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

Wochenbericht 3

meiner Bachelorpraxisphase

Jannis Priesnitz

26. April 2015

Zusammenfassung

Dieser Wochenbericht beinhaltet meine Tätigkeiten seit dem 27.03.2015 in dem Projekt „Sichere Kommunikation über CAN“ im Rahmen meiner Bachelor-Praxisphase bei Continental.

Inhaltsverzeichnis

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. (Das dies kein aus der Luft gegriffenes Problem ist zeigen die folgenden Quellen)

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 Bemühungen einer Verschlüsselung(it quelle CAN Vector) 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 die Machbarkeit. Hierzu werden sowohl gängige kryptografische Mittel ausgewählt um maximale Sicherheit zu gewährleisten, als auch Messungen an einer Untermenge mit geringerem Sicherheitsniveau (einem Subset an Sicherheit) von mir durchgeführt werden.

(Eigenleistung: Laufzeitmessung mit prototypischer Implementierung auf Testdevice.)

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.

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

Weiter soll die Frage geklärt werden, welche Mittel eingesetzt werden müssen, um ein maximales Sicherheitsniveau nach dem Stand der Technik einzusetzen. 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.
Ferner wird kurz auf die Hardwarevoraussetzungen eingegangen, die ein Kommunikationsteilnehmer mitbringen sollte, um die gewählten Algorithmen durchführen zu können.

4 Zielsetzung

Es soll untersucht werden, ob eine sichere Kommunikation über den CAN-Bus grundsätzlich möglich ist. Darüber hinaus soll auf die besonderen Randbedingungen bei einem Einsatz im automobilen Umfeld eingegangen werden. Außerdem sollen gängige kryptografische Mittel ausgewählt werden und deren Wahl kurz begründet werden. An einer prototypischen Implementierung eines Subsets sollen Messwerte genommen werden, anhand derer eine differenzierte Aussage über die Realisierbarkeit einer sicheren Kommunikation (nicht nur der Implementierten) getroffen werden kann.

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 mehrere Clients angehören.

6 Forschungsgegenstand

Sowohl das Feld der Kryptologie, als auch der Entwicklung von Software speziell für eingebettete Systeme waren Gegenstand vieler Forschungen. Arbeiten beschäftigen sich mit der sicheren Kommunikation über Geräte mit sehr wenig Leistung und über Schnittstellen, die über eine geringe Payload und lange Nachrichtenlaufzeiten verfügen.

Meine Aufgabe besteht darin, diese bereits gewonnen Erkenntnisse der beiden Systeme zusammen zu bringen und einen fundierten Überblick über die Möglichkeiten zu geben. Ein

weiterer wichtiger Aspekt [sind die Eigenschaften des CAN-Busses] ist das dem CAN zugrundeliegenden Multi-Master-Prinzip, weshalb nicht wie bei anderen Netzwerken von einer Ende zu Ende Kommunikation ausgegangen werden kann. ???

7 Methode

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

8 Materialübersicht

TBC

9 Vorläufige Gliederung

1. Einleitung / Hintergrund

   „Warum wird sichere Kommunikation im Auto benötigt:“

   Hackingangriffe auf Autos etc.

2. Aufgabenstellung

   „Was soll erreicht werden“

   Authentische Kommunikation

   Verschlüsselte Kommunikation

3. Randbedingungen der Automotive Embedded Welt und von CAN

   „Worauf muss im speziellen geachtet werden, wenn es im Auto laufen soll“

   Schwache System

   Wenig Speicher

   Ausfallsicherheit...

4. Konkretes Design

   „Wie habe ich mit gedacht, könnte man das lösen“

   RSA

   DeviceID als Passwort

   AES Domainen etc.

5. Performancemessungen

   „Die Messungen an der im Praktikum erstellten Software“

   Setup Zeit

   Lauftzeit einer Nachricht

   ggf. Speicher.

6. Fazit und Ausblick

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

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

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

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

11 Zeitplan

TBC