h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

Hochschule Darmstadt
- Fachbereich Informatik -

Sichere Kommunikation über das Controller Area Network (CAN)

Abschlussarbeit zur Erlangung des akademischen Grades
Bachelor of Science (B.Sc.)

vorgelegt von

Jannis Priesnitz
729341

Referent:	Prof. Dr. Ronald Moore
Korreferent:	Prof. Dr. Hans-Peter Wiedling

Abstract

Das Controller Area Network (CAN) ist ein umfassend standardisiertes System, was sich in vielen Anwendungsfällen in der Praxis, vor allem im Umfeld von Embedded Systems, bewährt hat. Trotz seiner Einschränkungen hinsichtlich Geschwindigkeit und nutzbarem Datenvolumen wird es bis heute in zahlreichen Systemen eingesetzt und ist immer noch Bestandteil neuer Entwicklungen. Dies ist u.a. auf die hohe Widerstandsfähigkeit gegenüber Störeinflüssen zurückzuführen.

Was passiert aber, wenn nicht nur informationstechnische Störungen vorliegen, sondern das Netzwerk von Angreifern kompromittiert wird? In einem gängigen CAN-Netzwerk kann jeder Teilnehmer beliebige Daten versenden, die von allen Teilnehmern ausgewertet werden. Dies kann zu schwerwiegenden Fehlfunktionen von technischen Anlagen führen.

Diese Arbeit beschäftigt sich mit der Frage, ob eine sichere Kommunikation über CAN grundsätzlich möglich ist, welche kryptografischen Algorithmen dafür besonders geeignet sind und welche Voraussetzungen an die Systeme gestellt werden müssen, um sicher zu kommunizieren. Des Weiteren wird der Vorschlag einer möglichen Softwareumsetzung in Form einer prototypischen Implementierung gemacht und anhand dessen Messungen durchgeführt. Mit Hilfe der Messergebnisse wird eine allgemeine Aussage über die Realisierbarkeit und den Aufwand einer sicheren Kommunikation getroffen.