Thesis

Reese + Techware
Technologie in Hard- + Software

Bachelor / Master

Thema: Entwicklung einer Software zur Umsetzung einer Chain of Trust auf einem Mikrocontroller

Immer mehr Industrie-Produkte werden gefälscht und das Reverse-Engineering von Firmware wird als Service angeboten – Bei immer mehr Baugruppen wird also der Schutz gegen solche Vorgänge interessant. Ein Lösungsansatz dafür ist die Authentifizierung von Hardware mittels einer Trusted Chain.

Aktuelle Controller unterstützen bei der Umsetzung mit umfangreichen Security-Features. Dadurch können wesentliche Aufgaben optimiert durch die Controller-Hardware übernommen werden.

Die Ziele dieser Arbeit sind:

- Konzeptionierung und Umsetzung einer Trusted Chain
- Bewertung der Effektivität des erreichten Schutzes und des Einsatzes hardwarebasierter Security-Features

Ansprechpartner: *Tobias Rastetter*
Tel. 048 21 / 900 67-33
tobias.rastetter@rxt.de

Grundsätzlich werden alle für die Arbeiten notwendigen Unterlagen und Hilfsmittel gestellt.