AutoCyberSec

Techniken aus dem Security Testing für die Bedrohungsmodellierung im Bereich Automotive

Programm / Ausschreibung	Qualifizierungsoffensive, Innovationscamps S, Innovationscamps S	**Status**	abgeschlossen
Projektstart	01.07.2022	**Projektende**	31.12.2022
Zeitraum	2022 - 2022	**Projektlaufzeit**	6 Monate
Keywords	automotive; iso21434; threatmodeling; security testing; penetration tests		

Projektbeschreibung

Im August 2021 wurde die ISO/SAE 21434 veröffentlicht. Diese beschreibt neue Anforderungen für die Cybersicherheit für elektrische und elektronische (E/E) Systeme. Für Unternehmen aus dem Automotive-Bereich ist dieser Standard eine neue Herausforderung: Komponenten in einem „road vehicle“ müssen mit Techniken aus dem Fachgebiet der Bedrohungsmodellierung analysiert werden und dem Stand der Forschung entsprechen. Die Techniken der Bedrohungsmodellierung analysieren ein technisches System bzw. eingesetzte Prozesse, um Risiken und Gegenmaßnahmen zu identifizieren. Diese Methodik gilt seit August 2021 und wird nun innerhalb der nächsten zwei Jahre für neue Fahrzeugtypen verpflichtend. Dies betrifft sowohl auch das Management-System, in dem die Sicherheitsrisiken verwaltet werden müssen.
Die Herausforderungen sind jedoch nicht nur technischer Natur, denn auch die Firmenkultur trägt hierzu einen wichtigen Beitrag. Bei der Entwicklung eines E/E Systems wirken verschiedene Rollen mit. In Unternehmen bilden sich erfahrungsgemäß Schwerpunkte um die technischen Themenbereiche (1) funktionale Sicherheit („Safety“, d.h. Schutz von Leib und Leben) und (2) technische Sicherheit („Security“, d.h. Schutz des Systems vor Sabotage und Missbrauch). Bisher lag der Fokus im Bereich der angewandten Ingenieurswissenschaften im Fahrzeugbau stark auf den Anforderungen von Verfügbarkeit und Safety (funktionale Sicherheit) und weniger auf Security. Da die unterschiedlichen Spezialisierungen von Safety und Security selbst sehr umfangreiches und detailliertes Domänenwissen erfordern, fehlt es in der Branche generell an Know-how. Dies bezieht sich sowohl auf Fahrzeughersteller als auch auf die Zulieferer von Teilen, Antriebssträngen und Elektronik. Dieses Innovationscamp hat die folgenden Ausbildungsschwerpunkte, welche die Entwicklung sicherer Produkte im Automotive-Bereich verbessern:
• Hintergründe und Vorgaben der ISO/SAE 21434, um die Cybersicherheit im Bereich Automotive Engineering nach geltenden Regulatorien abzubilden.
• Bedrohungsanalyse nach ISO/SAE 21434, um die Analysen und die zukünftigen Anforderungen auf Basis der Norm zu erstellen.
• Angewandte Testtechniken aus dem Bereich Penetration Testing, um Angriffe zu verstehen, die Qualitätssicherung auszubauen und effektive Gegenmaßnahmen zu entwickeln.
In diesem Projekt soll die Theorie des Standards ISO/SAE 21434 durch angewandte Hacking- und Security-Testing-Techniken

angreifbar und verständlich werden. Die Zielgruppe sind Mitarbeiter:innen aus dem Ingenieurswesen.

Projektkoordinator

- SBA Research gemeinnützige GmbH

Projektpartner

- eutema Research Services GmbH
- LieberLieber Software GmbH
- WOO Beteiligungs GmbH
- DigiTrans GmbH