



CYBERSICHERHEIT FÜR DAS VERNETZTE FAHRZEUG

FAHRZEUGE ALS SICHERHEITSRISIKO

Die Funktionen in einem modernen Auto werden immer mehr digitalisiert und das Fahren zunehmend automatisiert. In der Vergangenheit war das Auto ein isoliertes mechanisches Produkt, das nur durch direkten physischen Kontakt manipuliert oder gestohlen werden konnte. Heute werden praktisch alle funktionalen Teilsysteme eines Fahrzeugs von Software gesteuert und vernetzt.

Durch diese Digitalisierung und Vernetzung werden die Systeme komplexer und die Anzahl der potenziellen Angriffsmöglichkeiten steigt stark. Manipulation von Steuergeräten aus der Ferne, Ausspionieren von Positionsdaten des Fahrzeugs, Erstellung von Bewegungsprofilen von Fahrer:innen oder Knacken des

Fahrzeugfunkschlüssel-Systems und Zugriff auf die integrierte SIM-Karte - diese sind nur einige jener Gefahren, die von Hackern ausgenutzt und durchgeführt werden können.

Für das vernetzte Auto mit dessen zahlreichen Schnittstellen ist es daher unbedingt notwendig, sowohl Fahrzeug- als auch Nutzerdaten gegen unautorisierte Zugriffe zu schützen und alle Manipulationen jeglicher Fahrzeugfunktionen zu verhindern. In unserem Automotive Security Labor in Wien werden die Tests unter strengen Sicherheitsauflagen durchgeführt, welche die Einhaltung der hohen Sicherheitsanforderungen unserer Kunden gewährleisten.

SERVICES DES AIT AUTOMOTIVE TEST LABORS

Mögliche Schwachstellen werden durch gezielte automatisierte und manuelle Tests identifiziert. Mit Penetrationstests prüfen die AIT-Expert:innen Hardwarekomponenten, Schnittstellen, Anwendungen und Netzwerke rund um das vernetzte Fahrzeug. Unsere Expert:innen führen gezielte Angriffe durch, decken Sicherheitslücken auf und bewerten die Anfälligkeit Ihres Produkts bzw. Systems für Manipulationen. Reporting und die

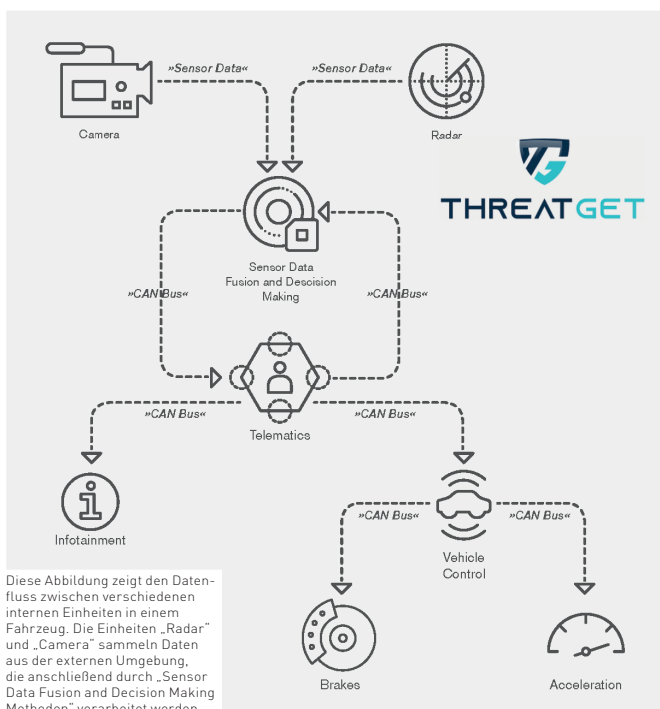
Dokumentation von Sicherheitslücken sowie Empfehlungen zur Risikominimierung runden das Leistungsspektrum ab. Die Tests werden in enger Zusammenarbeit mit unseren Kunden durchgeführt. Strenge Sicherheitsauflagen in unserem Testlabor garantieren, dass die Einhaltung der Sicherheitsanforderungen unserer Projektpartner gewährleistet ist.



TESTANSÄTZE UND METHODEN

Wir bieten folgende Services und Leistungen an:

- **Code- und Designanalyse**
 - Statische Code-Analyse
 - Erstellen von automatisierten Tests
 - Implementierung und Parametrierung der Tests
 - Unit Testing
- **Prüfung auf Robustheit**
 - Plausibilitätsprüfungen von Code und Daten
 - Value range scanning
 - Seitenkanal-Analyse
 - Analyse von Interfaces
- **Automatisiertes Security Assessment**
 - Das eigenentwickelte Tool ThreatGet identifiziert automatisch Bedrohungen und unterstützt das kontinuierliche Risikomanagement.
 - Teile von ThreatGet wurden in nationalen und internationalen Forschungsprojekten entwickelt (<https://www.threatget.com/>).
 - Eine kommerzielle Version von ThreatGet ist über die Lieber.Group erhältlich.
- **Vulnerabilitätsrecherche**
 - Umfangreiche weltweite Datenbanken (OpenVAS, Mitre CVE DB, ...)
- **Fuzz Testing**
 - Brute-force Fuzzer
 - Interface Scanning
 - Intelligent Analysis (bspw. Einsatz von KI-Technologien)
- **Penetration Tests**
 - DoS
 - Replay attack
 - Generated messages
 - Manipulated messages
- **Regressionstests**
 - Automatisierte Tests nach HW / SW updates
- **Erstellung von Testreports**
 - Zusammenfassung der durchgeführten Tests und Testergebnisse



Diese Abbildung zeigt den Datenfluss zwischen verschiedenen internen Einheiten in einem Fahrzeug. Die Einheiten „Radar“ und „Camera“ sammeln Daten aus der externen Umgebung, die anschließend durch „Sensor Data Fusion and Decision Making“ verarbeitet werden.

Die Datenübermittlung erfolgt an eine „Telematics“, die die Verfolgung des Fahrzeugs steuert. Die Telematik interagiert mit der zentralen „Vehicle Control“, um die Geschwindigkeit des Fahrzeugs entweder durch „Brakes“ oder durch „Acceleration“ zu steuern. Das „Infotainment“ verbindet sich mit der Telematik, um dem Fahrer Informationen zur Verfügung zu stellen.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

DI Dr. Stefan Schauer

Tel +43 50550-4055

Giefinggasse 4, 1210 Wien

stefan.schauer@ait.ac.at

www.ait.ac.at/dse