OPTIMAbit
Automotive Pentests

IHRE VORTEILE

- → Maßgeschneidertes Angebot für die Anforderungen eines Automotive OEMs bzw. Zulieferers.
- → Pentests vom einzelnen Steuergerät über Verbundsysteme (bspw. Wegfahrsperre) bis hin zum Gesamtfahrzeug und seinem Ecosystem (Produktion, Apps, Cloud Anbindung/ Backend, Customer Services)
- → Erfahrung mit allen relevanten Technologien:
  - Busse (CAN, LIN, FlexRay, MOST, ...)
  - Funk (Wifi, BT+BTLE, NFC, GSM, ...)
  - Low-Level (JTAG, UART, I2C, etc.)
  - Restbus-Simulation

WANN IST EIN AUTOMOTIVE PENTEST RATSAM?

- → Sicherstellen, dass Insassen vor Gefahren für Leib und Leben geschützt sind
- → Verhinderung von Diebstahl persönlicher Daten
- → Sicherstellen der Verfügbarkeit und Zuverlässigkeit für eine perfekte Driver Experience
- → Als Abnahmekriterium für einen OEM oder Zulieferer

DAS AUTONOME UND VERNETZTE FAHRZEUG IST DIE ZUKUNFT UND GLEICHZEITIG EIN KOMPLEXES RISIKO. JETZT DURCH SECURITY TESTS ABSICHERN!

Moderne Fahrzeuge gehören heute zu den komplexesten IoT Geräten. Ob mit oder ohne autonomes Fahren sind Autos absolute High-Tech-Geräte mit unzähligen Bus-Systemen, zahlreichen ECUs und verschiedenen Funkverbindungen zur Infrastruktur, anderen Verkehrsteilnehmern und ins Internet. Die Angriffsfläche ist groß und die Möglichkeiten Angriffe während der Fahrt zu erkennen und abzufangen, begrenzt. Ein erfolgreicher Angriff kann „nur“ ein Ärgernis für den Kunden sein, jedoch auch verheerende Folgen für das Unternehmen und die physische Sicherheit der Insassen des Fahrzeuges haben.

Im Rahmen des Pentests einer ECU oder eines Gesamtfahrzeuges analysieren wir die Angriffsfläche der Geräte bzw. des Fahrzeuges und prüfen eingesetzte Härtungs-Maßnahmen gegen lokale und externe Manipulationen und liefern Ihnen einen ausführlichen Bericht, der Ihnen hilft, die erkannten Schwachstellen in Ihr Unternehmen zu tragen und wirkungsvoll zu bekämpfen.

Von typischen Pentests im Web- und (IT-)Infrastrukturbereich unterscheiden sich IoT und Automotive Pentests insbesondere durch den physischen Zugriff des Angreifers auf das Angriffsobjekt. Die Experten der OPTIMAbit sind dafür ausgebildet, bis auf unterster Hardware-Ebene Härtungs-Maßnahmen zu prüfen und zu untersuchen. Auf Wunsch auch Tamper-Proof Maßnahmen, wie Vergießen, Versiegeln oder HW-Fusing.

OPTIMAbit GmbH
Kaflerstr. 6 | 81241 München
+49 89.88951819-0 | service@optimabit.com

INFORMATION SECURITY CONSULTING & TESTING
FERNAO DIVISION

OPTIMAbit