Car-Forensics 5.0

Dipl.-Ing. Thomas Käfer, M.Sc.

Dipl.-Ing. M.Sc.
Thomas Käfer
EDV Sachverständiger



www.car-forensics.de

Seminar Automotive Security

Digitale Kfz-Forensik, Datensicherheit und -schutz im Kontext von Fahrzeugvernetzung und Functional- und Road-Safety

Seminar Car-Forensics – Automotive Security 5.0

Motivation: Durch die zunehmende Vernetzung von Fahrzeugen untereinander, mit Smartphones und zentralen Infrastrukturen (Car2X) sowie durch Erweiterungen wie Unfalldatenschreibern und das System „eCall“ bis hin zum automatisierten und autonomen Fahren muss der Fokus von reinen Fragen der Functional- und Road-Safety mehr und mehr in Richtung auf IT-Sicherheitsaspekte (Security) und Datenschutz (Privacy) erweitert werden. Das Bewusstsein über die Gefahren, die durch mangelhafte IT-Sicherheit im Automotive-Umfeld ausgehen, hat sich durch die zahlreichen Incidents und Veröffentlichungen ab 2015 spürbar verändert. Dennoch ist in vielen Bereichen der Automobilindustrie und Automotivszene die Komplexität der Herausforderung für sichere IT-Systeme im und um das Fahrzeug herum noch nicht adäquat erkannt worden bzw. findet in den Produkten und Services keine ausreichende Beachtung.

Die Speicherung und der Austausch von Fahrzeug- und Bewegungsdaten wecken Begehrlichkeiten bei Industrie, Polizei und Justiz, Versicherungen und Dienstleistern aber auch bei Kriminellen. Aus der Vernetzung und Steuerungsmöglichkeit von Fahrzeugen via Funk ergeben sich komplett neue Bedrohungsszenarien im Bereich der IT-Security mit Auswirkungen auf die Functional- und Road-Safety.

Probleme der IT an sich und mit deren Sicherheit werden durch Schwachstellen verursacht, deren Ursache fast immer mit menschlichen Fehlern zusammenhängt. Je mehr Fehler Menschen bei der Entwicklung, Integration, Administration oder Nutzung von IT machen, desto mehr Schwachstellen gibt es und umso größer ist das Risiko von Fehlfunktionen oder erfolgreicher Angriffe. Im Zeitalter der Digitalisierung kann dem nur gegengesteuert werden, wenn die Gründe für Schwachstellen – die Fehler der beteiligten Menschen – reduziert werden. Dabei ist die Sichtweise des Hackers dem Ingenieur üblicherweise vollkommen fremd. Dem kann durch das Seminar abgeholfen werden. Denn: IT-Sicherheit und Datenschutz werden von Entwicklern und Treibern der Digitalisierung oft als Hemmnisse und Stolpersteine auf dem Weg zu einer schnellen Lösung gesehen. Der Versuch, diese Punkte in fast fertige Produkte nachträglich zu integrieren oder gar „hinein zu testen“, ist zum Scheitern verurteilt bzw. erhöht die Entwicklungskosten erheblich (bei gleichzeitig geringerer Produktqualität). Tatsächlich sind sogenannte Penetration-Tests nur ein Baustein, um am Ende (regelmäßig) zu prüfen, ob das geforderte Schutzniveau auch erreicht wird.

Viele Schäden könnten von Beginn an verhindert werden, wenn den beteiligten Entwicklern und Entscheidern ein Basiswissen an IT-Sicherheit vermittelt würde. Andere können durch den Einsatz von IT-Sicherheitsexperten in wichtigen Phasen von IT-Projekten erkannt und beseitigt werden. Tatsächlich sind IT-Sicherheit und Datenschutz als integrale Bestandteile einer jeden IT-Entwicklung bereits in der Konzeptionsphase der Idee zu berücksichtigen. Das senkt nicht nur die Entwicklungskosten für diese Punkte, sondern zeigt bereits in einem frühen Stadium, ob und wo die Geschäftsidee aus Security- oder Datenschutz-Sicht angreifbar ist.

Betrachtet man, wie unbedarft und fahrlässig aktuelle Systeme und Netzwerke gerade im Bereich von Automobilen aber auch bei Industriesteuerungen, Web-Anwendungen, Smart-Home und Stromversorgungsnetzen aktuell bzw. in der jüngeren Vergangenheit entwickelt wurden, ist das Vertrauen in deren Betriebs- und IT-Sicherheit unbegründet.

Ein Ausfall bzw. Angriff auf solch ein System produziert nicht nur erhebliche Kosten und Schäden, sondern senkt die Reputation des Anbieters auf ein ggf. existenzbedrohendes Niveau. Für den Nutzer kann ein IT-Security-Incident letztlich tödlich enden.

Anhand von zahlreichen aktuellen Beispielen lassen sich konzeptionelle und individuelle Fehler sehr plastisch demonstrieren. Nach dem Motto „Niemand ist unnütz – er kann immer noch als schlechtes Beispiel dienen“ kann man daran nicht nur die Risiken demonstrieren, sondern auch geeignete Abhilfemaßnahmen diskutieren, um die Eintrittswahrscheinlichkeit derartiger Vorfälle deutlich zu senken.

Am Ende bleibt ein Rest-Risiko, das es zu bewerten und zu minimieren gilt. Hier sind vor allem die Risiken, die eine hohe Eintrittswahrscheinlichkeit gepaart mit einer hohen Schadensauswirkung haben, bevorzugt zu betrachten.

Security by Design und Privacy by Design sollten daher nicht nur leere Marketing-Schlagworte oder Normen wie beispielsweise der DS-GVO geschuldet sein, sondern tatsächlich belastbare Qualitätskriterien jeder modernen Digitalisierungsstrategie und IT-Entwicklung.

Seminarkonzept: Das Seminar „Car-Forensics – Automotive Security“ basiert auf und orientiert sich an der gleichnamigen Forschungsarbeit (Stand 05/2019 ISBN: 9783738635393) und soll vorgenannten Aspekten Rechnung tragen und zeigen, was technisch im Bereich der digitalen forensischen Auswertung der in den Kfz verbauten bzw. extern mit den Fahrzeugen gekoppelten IT-Systemen derzeit bereits möglich und zukünftig denkbar ist. In diesem Kontext wird beleuchtet, welche Rechtsgrundlagen zurzeit vorhanden und anwendbar sind und wo nach wie vor Regelungsbedarf seitens des Gesetzgebers besteht. Im praktischen Teil wird thematisiert, welche Schnittstellen die verschiedenen Systeme besitzen, die forensisch angesprochen bzw. ausgewertet werden können. Hierbei wird sowohl auf offen kommunizierte Standards und Zugänge zugegriffen als auch z.B. mittels Hacking- und Analysewerkzeugen mit Hilfe von Reverse-Engineering-Methoden eine Datenauswertung bzw. -manipulation gezeigt. Mittels Vorgehensweisen der digitalen Forensik und typischer Angreifer wird an Beispielen aus dem Automotive-Umfeld und dem Internet der Dinge visualisiert, inwieweit technische und organisatorische Sicherungen umgangen werden können bzw. welche Daten tatsächlich übertragen und gespeichert werden.

Zielsetzung: Im Seminar werden die Themen Datensicherheit und -schutz aus Sicht der Betreiber und Verwender sowie die forensischen Möglichkeiten und Rechte für Sachverständige und Ermittler beleuchtet. Des Weiteren wird ein Code of Conduct für Car2X-Kommunikation diskutiert. Die Erkenntnisse aus den verschiedenen Angriffsszenarien und Werkzeugen der Hacker können von mit der Entwicklung betrauten Ingenieuren wiederum verwendet werden, um die Systeme nicht nur in Hinblick auf die funktionale Safety sondern auch und vor allem auf die IT- und Daten-Sicherheit (Security) zu härten.

Zielgruppe: Das Seminar richtet sich gleichermaßen sowohl an Entwickler und Betreiber von Automotive-Systemen (Hard- und Software) als auch an Entscheider, die Personal- und Entwicklungsverantwortung in diesem Bereich tragen (OEM und Zulieferer) sowie Verbände und Behörden. Für die unterschiedlichen Zielgruppen werden separate Workshops mit differenziertem Gesamtumfang und fachlicher Tiefe angeboten (1/2 Tag, 1 Tag und 2 Tage).

Voraussetzungen: Vorkenntnisse im Bereich der Software- und System-Entwicklung sowie der IT-Sicherheit sind wünschenswert, jedoch nicht zwingend erforderlich. Im Seminar wird versucht, das Themenfeld Car-Forensics in der Breite und dort wo nötig und sinnvoll in der erforderlichen Tiefe zu betrachten und eine für alle Teilnehmer verständliche Fachsprache zu verwenden.

Kosten: Die Kosten für ein Seminar bzw. einen Workshop differieren entsprechend der gewünschten Dauer, des Schulungsortes und des ggf. individuell angepassten Inhalts oder der Schwerpunktsetzung. Auf Anfrage erhalten Sie gerne ein konkretes Angebot incl. aller Spesen.

Vertraulichkeit / NDA: Der Referent ist bereits aufgrund seines Berufsstandes als ö.b.u.v. Sachverständiger zur Vertraulichkeit verpflichtet. So werden in den Schulungen weder Namen oder Details aus anderen Kundenprojekten kommuniziert noch werden konkrete Wortbeiträge oder Meinungen der Seminarteilnehmer aus den Diskussionen in anderen Schulungen weiter verbreitet. Erfolgt über die reine Wissensvermittlung eine individuelle Projektberatung, so ist der Abschluss eines NDA möglich.

Projektbetreuung: Auch bzw. gerade nach der Schulung steht Ihnen der Referent Thomas Käfer als kompetenter Ansprechpartner rund um die Themen IT-Sicherheit, Forensik und Datenschutz im Rahmen von Projekt- und Entwicklungsunterstützung auf Honorarbasis zur Verfügung. Seine Tätigkeiten können sowohl beratender Natur bei der Konzeption von fahrzeugnahen IT-Systemen sein als auch deren nachfolgende Bewertung z.B. im Rahmen von Security- und Privacy-Audits und Penetration-Tests beinhalten.

Vorstellung Referent: Dipl.-Ing Thomas Käfer, M.Sc. ist mit seinem IT-Systemhaus seit 1990 selbstständig in der IT tätig. Das Tätigkeitsfeld der Firma Käfer umfasst Consulting-Leistungen im Bereich der IT-Sicherheit incl. Penetration-Testing u.a. im Automotive-Umfeld. Thomas Käfer arbeitet seit 2002 als Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung (seit 2006 öffentlich bestellt), als IT-Consultant, Fachautor und beschäftigt sich vor allem mit Fragen der IT-Sicherheit, dem Datenschutz und dem Gebiet der Digitalen Forensik. Ehrenämter als Handelsrichter am Landgericht Aachen sowie als Mitglied der Vollversammlung der IHK Aachen (Ausschüsse Industrie und Technologie, Außenhandel sowie Berufsbildung) komplettieren seine Tätigkeiten. Er hat 2015 erfolgreich den berufsbegleitenden Masterstudiengang „Digitale Forensik“ als Zweitstudium an der Hochschule Albstadt-Sigmaringen in Kooperation mit der LMU München und der FAU Erlangen abgeschlossen und in diesem Rahmen eine umfangreiche Forschungsarbeit zum Thema Digitale Kfz-Forensik erstellt. Thomas Käfer beschäftigt sich regelmäßig mit Fragestellungen der IT-Sicherheit und der forensischen Auswertung von modernen Fahrzeugen und IT-Systemen, die mit diesen gekoppelt werden. Er ist Speaker auf Veranstaltungen zum Thema IT-Sicherheit und Datenschutz und hält Workshops zu diesem Thema für Automobilindustrie, Zulieferer, Behörden und Verbände und ist Mitglied der Fokus-Gruppe IT-Security im Digital Hub Aachen.



Dipl.-Ing. Thomas Käfer, M.Sc. – Elchenrather Weide 20 – D-52146 Würselen
Tel. 02405/47949-0 – E-Mail: Kaefer@Kaeferlive.de – www.Car-Forensics.de

Veröffentlichungen und Medienberichterstattung (auszugsweise)

- 08.10. bis 10.10.2018 Car Forensics auf dem 27. Aachener Fahrzeug- und Motorenkolloquium von FKA und IKA der RWTH Aachen
- Car-Forensics beim Science-Link: Networking 4.0 "Datensicherheit bei autonomem Fahren" am 19.03.2018 in Aachen



- 18.11.2016: Vortrag Car-Forensics beim VDI/VDE in Frankfurt/Main
- Speaker auf der IT-Security-Messe Leetcon Hannover im November 2016
- Wirtschaftliche Nachrichten der IHK Aachen 11/2016
- 08.09.2016: Speaker Car-Forensics 11. Dortmunder Autotag
- Speaker auf dem 25. Aachener Kolloquium Fahrzeug- und Motorentechnik der RWTH Aachen - Vortrag zur IT Sicherheit im Kfz Oktober 2015 und 2016
- Speaker auf dem IT-Security Breakfast der IHK Bonn September 2016
- 11.12.2015: Aachener Interdisziplinäres Verkehrssymposium
- 02.12.2015: IT Sicherheit Industrie 4.0 auf dem IT-Sicherheitstag NRW
- 06.11.2015: Speaker Car-Forensics beim IT Security Breakfast Bonn
- 21.-22.10.2015: Poster Car-Forensics auf der Automotive Security 31. VDI/VW-Gemeinschaftstagung in Wolfsburg
- Berufsporträt Digitaler Forensiker in den VDI Nachrichten vom 09.10.2015
- 06.10.2015: Hausmesse Wolfsburg - Vortrag zur IT Sicherheit im Kfz
- ARD Tagesschau und WDR Aktuelle Stunde Stellungnahme zur VW-Abgassoftware (22.09.15 und 25.09.2015)
- ARD Plusminus extra Stellungnahme zur VW-Abgassoftware (21.09.2015)
- MDR Fakt ist…! BMW Hack (21.09.2015)
- Selbst ist das Auto in der FAZ vom 06.09.2015



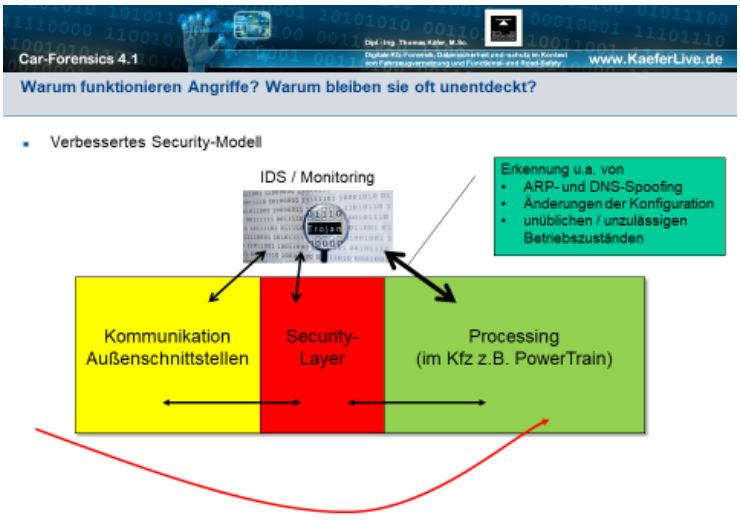
- ARD tagesthemen vom 23.07.2015 zum Jeep-Hack / BMW-Hack
- Berufsbild Digitale Forensik in der Südwest Presse und Stuttgarter Zeitung
- 12.05.2015: Speaker IT-Forensik-Workshop an der FH-Aachen
- WDR-Fernsehen Lokalzeit Aachen vom 08.05.2015
- Car-Forensics in der Zeitschrift Mobile Business 03-2015
- 16.03.2015 - 20.03.2015: CeBIT – Speaker Car-Forensics
- 03.12.2014: Speaker IT Sicherheit Hagen - IT-Sicherheitstag NRW 2014
- 24.11.2014: Speaker Digitale Kfz-Forensik - Köln - cologne IT summit
- 16.09.2014: Speaker Car-Forensics 9. Dortmunder Autotag

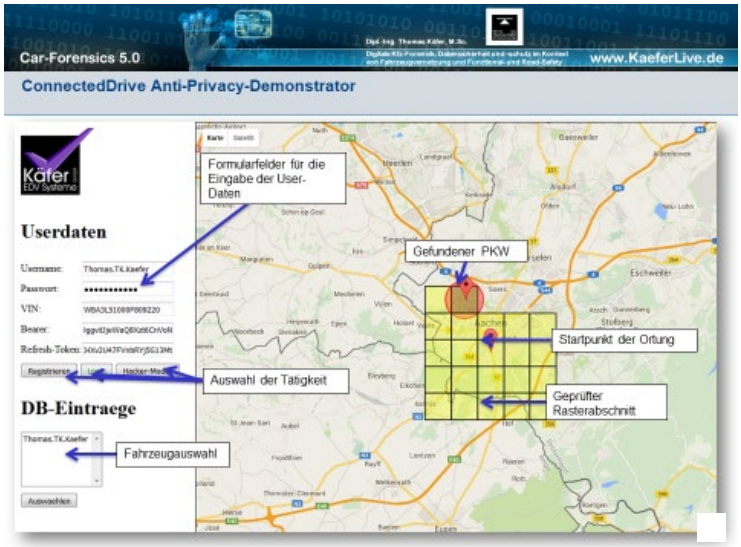
Seminargliederung Ein- und Zwei-Tagesseminar: Beim Zwei-Tagesseminar erfolgt eine Vertiefung der einzelnen Aspekte. Der Workshop lädt zum Mit-Diskutieren ein und die Themen werden nicht trennscharf sondern in der Gesamtheit und mit ihren Wechselwirkungen übergreifend betrachtet. Der Workshop basiert auf der aktuellen Ausgabe der Forschungsarbeit Car-Forensics 5.0 von Mai 2019. Je nach Umfang des Seminars und Zielgruppe wird der Fokus bzw. die Detailtiefe angepasst (Beispiel unterschiedliche Schwerpunkte und Tiefgang für Entscheider, Entwickler oder Forensiker/Ermittler). Das aktuelle Material umfasst ca. 460 Folien.

1. Vorstellung und Motivation
    - Vorstellung: Was ist und was leistet die Digitale Forensik?
    - Herausforderungen der Digitalen Transformation
    - Einführung ins Thema Cybersicherheit und Datenschutz
    - Vorstellung der Forschungsarbeit Car-Forensics
2. Digitale Verschlüsselung, Zertifikate und digitales Signieren
    - Grundlagen
    - Angriffsszenarien
    - Konkrete Umsetzungsempfehlungen
3. Digitale Kfz-Forensik: Vorstellung der Forschungsergebnisse
    - Gefundene Schwachstellen (Datenschutz) am Beispiel eCall und Unfalldatenschreiber
    - Angriffsflächen von Fahrzeugen incl. gefundener Schwachstellen in Bezug auf IT-Security
    - Fehlfunktionen und Unzulänglichkeiten von IT- und Assistenz-Systemen im Fahrzeug in Bezug auf Funktion, Zuverlässigkeit und funktionaler Sicherheit
    - Konkrete Vorgehensweise für forensische Untersuchungen und Pen-Tests an Fahrzeugen und fahrzeugnahen Systemen
    - Diskussion geeigneter Event-Data-Recorder im Spannungsfeld von Aufklärung und Privacy
    - Auswertung Uber Crash mit Todesfolge in Tempe, Arizona incl. Erkenntnissen für Zuverlässigkeit von automatisiert fahrenden Fahrzeugen und deren Tests auf öffentlichen Straßen
4. Normen und gesetzliche Vorgaben
    - Welche Gesetze sind anwendbar?
    - Wiener Übereinkunft, STVO, STVG
    - Welche Normen passen in Bezug auf IT-Sicherheit und Privacy?
5. Allgemeine Digitale Forensik
    - Wie Angriffe im Netzwerk und auf schlechte Software funktionieren (z.B. MITM, Arp-Spoofing, Phishing und Bufferoverflows)
    - Empfehlungen für bessere Software- und System-Entwicklung
    - Vorgehensmodelle unter Berücksichtigung von IT-Security und Privacy
    - Test-Methoden und Qualitätsmanagement (u.a. richtiges Pen-Testing)
6. Datenschutz und Privacy
    - Die DS-GVO und die Auswirkung auf die Automobilbranche
    - Negativ-Beispiele und Herausforderungen
7. Incident Response und Best Practice Sicherheitsempfehlungen
8. Fazit und Diskussion

Impressionen aus dem Seminar:







Impressionen aus dem Seminar:

