Digitale Forensik

Dipl-Ing. Thomas Käfer

Forschungsarbeit Car-Forensics

Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung

www.KaeferLive.de

Forschungsarbeit „Car-Forensics“

Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung

1 Inhalt

Kontaktdaten: **Käfer EDV Systeme GmbH**
Dipl.-Ing. Thomas Käfer
Elchenrather Weide 20
52146 Würselen
Tel. 02405/479490

info@car-forensics.de
http://www.car-forensics.de

Stand: 24.02.2015

2 About

Die zunehmende Vernetzung von Fahrzeugen untereinander (Car2Car), mit Smartphones (Car2Phone) und zentralen Infrastrukturen (Car2Infrastructure) sowie optional bzw. zukünftig verpflichtend in KFZ zu implementierenden Erweiterungen wie Unfalldatenschreibern und das System „eCall“ sind unter IT-Sicherheitsaspekten und Datenschutzbetrachtungen bisher weitestgehend unerforscht. Die Speicherung und der Austausch von Fahrzeug- und Bewegungsdaten wecken Begehrlichkeiten bei Polizei und Justiz (z.B. im Rahmen von Verkehrsüberwachung und -delikten, Strafverfolgung sowie Unfallrekonstruktion), Versicherungen, und Dienstleistern, aber auch Kriminellen.

Die Masterthesis "Car-Forensics" im Rahmen des Studiengangs "Digitale Forensik" an der Hochschule Albstadt Sigmaringen (in Kooperation mit der Friedrich-Alexander-Universität Erlangen und der Ludwig-Maximilians-Universität München) soll einen ersten Überblick liefern, 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 soll beleuchtet werden, welche Rechtsgrundlagen zurzeit vorhanden und anwendbar sind und wo für die nahe Zukunft Regelungsbedarf seitens des Gesetzgebers besteht. Hierzu sollen im theoretischen Teil der Arbeit u.a. die geltenden Normen, Verordnungen und Standards sowohl unter rechtlichen als auch unter technischen Aspekten mit den Anforderungen an Datenschutz und Datensicherheit abgeglichen werden.

Im praktischen Teil der Masterthesis soll recherchiert und geprüft werden, welche Schnittstellen die verschiedenen Systeme besitzen, die forensisch angesprochen bzw. ausgewertet werden können. Hierbei soll sowohl auf offen kommunizierte Standards und Zugänge zugegriffen als auch z.B. mittels Hacking- und Analysewerkzeugen ggf. mit Hilfe von Reverse-Engineering-Methoden eine Datenauswertung bzw. -manipulation versucht werden. U.a. mittels Vorgehensweisen wie Social Engineering, der digitalen Forensik und typischer Angreifer soll an Beispielen geprüft werden, inwieweit technische und organisatorische Sicherungsmaßnahmen umgangen werden können, um Zugangssicherungen auszuhebeln bzw. welche Daten tatsächlich übertragen und gespeichert werden. Infrastrukturen, z.B. im Bereich Car-Sharing, e-Mobility und Verkehrsleitsystemen, bedürfen einer weiteren Betrachtung hinsichtlich ihrer forensischen Auswertbarkeit / Relevanz und der IT-Sicherheit.

Zielsetzungen der Masterthesis sind somit u.a., Aussagen über den Datenschutz und die Datensicherheit aus Sicht der Verwender (Benutzer) zu treffen, die forensischen Möglichkeiten und Rechte für Sachverständige und Ermittler zu beleuchten und einen Code of Conduct für Car2Car-, Car2Infrastructure- und Car2Person-Kommunikation zu definieren.

Der Autor – Dipl.-Ing. Thomas Käfer – absolviert derzeit den berufsbegleitenden Masterstudiengang Digitale Forensik an der Hochschule Albstadt-Sigmaringen in Kooperation mit der LMU München und der FAU Erlangen und befasst sich in seiner alltäglichen beruflichen Tätigkeit seit vielen Jahren mit den Themen Datenschutz und IT-Sicherheit.

3 Use-Cases und konkrete Forschungsansätze

Im Rahmen der Forschungsarbeit sollen folgende Themenfelder bearbeitet werden:

- **Angriffsszenarien für Automotiv-Smartphone-Apps:** Durch die Kopplung von Smartphones und deren Apps mit modernen Fahrzeugen gibt es Möglichkeiten, Kfz-Infrastrukturen indirekt anzugreifen. So soll z.B. geprüft werden, ob gängige Navigations-Apps Geo-Daten loggen und ob man mit herstellerspezifischen Apps Fahrzeuge unberechtigt auslesen, öffnen oder gar starten kann.
- **Betriebssicherheit von Kfz (Safety Critical):** Welche Manipulationsmöglichkeiten von sicherheitsrelevanten Steuergeräten zur Provozierung von Unfällen gibt es und welche Maßnahmen ergreifen die Kfz-Hersteller, um das Einschleusen von Schadcode (Trojaner) zu verhindern bzw. mindestens zu erschweren? Gibt es Ansätze, Unfälle durch gezieltes Hacken von Kfz zu provozieren (vgl. sogenannte „Autobumser“, die Unfälle zum eigenen Vorteil verursachen)?
- **IT-Sicherheit (Security Critical) bei Kfz und Car-Kommunikation**: Am Beispiel von Systemen wie „Audi Connect“, „BMW ConnectedDrive“ und „Mercedes Connect Me“ soll geprüft werden, welche Daten vom Fahrzeug an den Hersteller oder Dritte übertragen werden, ob und wie man diese Kommunikation mitlesen, kopieren und manipulieren kann und ob es Möglichkeiten gibt, z.B. WLAN-Car-Hotspots und Bluetooth-Verbindungen zu kompromittieren.
- **Car2X**: Mit Car2X bzw. Car2Infrastructure bezeichnet man jegliche Kommunikation des Fahrzeugs zu IT-Infrastrukturen, die von den Automobilherstellern oder Drittanbietern zur Verfügung gestellt werden (und umgekehrt). Hierbei übertragen Kfz z.B. ihre aktuelle Position und Geschwindigkeit an Verkehrsdienstdatenbanken (vgl. RTTI, HD-Traffic u.a.), die somit ein sehr aktuelles und genaues Bild der Verkehrslage prinzipiell auf allen Straßen für andere Nutzer bereitstellen können. Unklar ist, welche Daten übertragen, ob diese Daten vollständig anonymisiert und ob sie für einen längeren Zeitpunkt gespeichert und durch die Dienstanbieter weiterverarbeitet werden (können).
- **Car2Person:** Zur Erhöhung der Sicherheit von Fußgängern planen Automobilhersteller, Fußgänger mit Transpondern auszustatten, die im Nahbereich mit entsprechend ausgestatteten Kfz kommunizieren können, um gefährliche Verkehrssituationen (z.B. Verdecken einer Person hinter einem parkenden Fahrzeug) schon in der Entstehungsphase zu vermeiden oder abzumildern. Die Frage stellt sich, ob hierbei Daten gespeichert werden und ob die Kommunikation anonymisiert erfolgt.
- **Car2Car:** Zur Erhöhung der Verkehrssicherheit werden Fahrzeuge zukünftig untereinander automatisiert kommunizieren und Daten austauschen. Interessant im Sinn der Betriebssicherheit und des Datenschutzes ist, ob diese Kommunikation protokolliert wird und ob der Austausch vollständig anonymisiert erfolgt bzw. kompromittiert werden kann. Wird es Möglichkeiten für die Verkehrsüberwachungsbehörden geben, diese Daten im Rahmen der Ordnungswidrigkeitenverfolgung auszulesen (Entfall von Radaranlagen)?
- **Unfalldatenschreiber:** Es besteht die Möglichkeit, derzeit weitestgehend auf freiwilliger Basis, Unfalldatenschreiber in Kfz zu verbauen, die bei einem Unfall Rückschlüsse auf Geschwindigkeit, Wegstrecke, Beschleunigungs- und Bremsvorgänge, gesetzte Blinker etc. erlauben.

Diese Daten können für den Fahrer belastend oder entlastend sein. Zu klären ist u.a., ob der Fahrer das Recht und die Möglichkeit hat, die Daten vor einer Verwendung durch Ermittlungsbehörden selber einzusehen und ggf. zu löschen bzw. ob die Daten manipulationssicher im Speicher abgelegt werden. Des Weiteren ist zu prüfen, ob sich aus den Daten längerfristige Bewegungsprofile erstellen lassen.

- **Automatisches Notruf-Systeme eCall**: Hierbei handelt es sich um ein ab Oktober 2015 in alle in der EU neu zugelassenen Fahrzeuge (PKW und leichte Nutzfahrzeuge) zu verbauendes Notrufsystem, welches im Fall eines Unfalls automatisiert (oder manuell) einen Anruf über die einheitliche Rufnummer 112 tätigt. Mittels Schnittstellen zum Fahrzeug können weitere Daten zur Schwere des Unfalls übermittelt werden (ausgelöste Airbags, Anzahl der besetzten Sitze usw.). Es ist in der Öffentlichkeit derzeit unbekannt, welche Daten hierbei aufgezeichnet und übertragen werden und ob ggf. Dritte (Abschleppdienste, Versicherer, Autohersteller usw.) diese Daten erhalten. Erste Diskussionen in der Öffentlichkeit lassen darauf schließen, dass es seitens der Verwender/Bürger eine hohe Skepsis gibt, ob hierbei auch Daten aufgezeichnet werden, die sich ggf. unabhängig von einem Unfall forensisch auswerten lassen (z.B. Ordnungswidrigkeitenverfolgung, Erstellung von Bewegungsprofilen).
- **Haftungsfragen und Datenschutz beim automatisierten Pilotieren von Kfz:** Sobald Kfz es erlauben, dass der Fahrer zeitweise oder vollständig von der Aufgabe entbunden wird, das Auto selbst zu steuern oder zu überwachen, muss allein aus Haftungsfragen sichergestellt werden, dass jeweils protokolliert wird, ob der Fahrer oder die Maschine das Fahrzeug gesteuert bzw. beaufsichtigt hat, wenn ein Unfall oder ein Verkehrsverstoß eingetreten ist. Hierzu bedarf es z.B. einer Aufzeichnung der Aktivitäten des Fahrers über eine Innenkamera, um zu protokollieren, ob der Fahrer aufmerksam war oder geschlafen bzw. ob er aktiv in das Geschehen eingegriffen hat. Das berührt u.a. das Recht am eigenen Bild sowie Datenschutzfragen und die Frage, wer nachher auf diese Daten wie zugreifen kann und darf. Sollte ein autonom fahrendes Fahrzeug einen Verkehrsverstoß oder gar einen Unfall (ggf. mit Personenschaden) verursacht haben, stellt sich die Haftungsfrage (Zulieferkette) und wer ggf. strafrechtlich belangt wird (vgl. Ahnung mit Freiheitsstrafe).
- **Notwendige Rechtsreformen für automatisiertes Pilotieren von Kfz:** Im Rahmen des automatisierten Pilotieren von Kfz müssen geltende Rechtsnormen an die neuen Anforderungen angepasst werden (vgl. u.a. Wiener Abkommen). Zu klären ist zudem, welche Datenschutznormen ggf. angepasst werden müssen (u.a. ob Fahrzeugdaten personenbezogene Daten sein können, wie z.B. die IP-Adresse eines Computers)
- **Logs von Navigations- und Steuerungsgeräten:** Vollkommen unerforscht bzw. öffentlich bekannt ist, ob und welche Daten in fest eingebauten Navigations- und Steuergeräten langfristig gespeichert werden (z.B. GPS-Daten), ob diese (und wenn ja, von wem) extern ausgelesen und forensisch ausgewertet werden können und dürfen. Zu prüfen ist, ob diese Daten gelöscht und ob gelöschte Dateien wieder hergestellt werden können.
- **Zugriffsmöglichkeit auf Steuergeräte über OBD/CAN-Bus:** Auch technisch soll betrachtet werden, welche Daten über welche Schnittstellen übertragen werden können. Gibt es beispielsweise Möglichkeiten, auf die Daten einer Frontkamera bei Unfällen zuzugreifen?

Welche Zugriffsmöglichkeiten und Sicherungen bestehen bei der OBD-Schnittstelle und dem/den CAN-Bussen? Die Hersteller lassen jedoch i.d.R. nur den Zugriff auf die Steuergeräte bzw. Sicherheitsebenen zu, die im Rahmen von Hauptuntersuchungen offen gelegt werden müssen. Unklar ist, ob diese Zugänge auf Weisung eines Richters für Ermittlungsbehörden und Sachverständige weiter geöffnet werden müssen bzw. wie das technisch/organisatorisch vollzogen werden soll.

- **Qualitätssicherung von in Kfz eingesetzter Soft- und Hardware**: Nach Aussage der Automobilindustrie ist damit zu rechnen, dass die Software in modernen teil- bzw. vollautomatisiert pilotierten Kfz ca. 100 Mio. Zeilen Code enthalten wird. Das ist ein Vielfaches des Umfanges beispielsweise von Smartphone-Betriebssystemen (Android ca. 12 Mio. Zeilen Code) oder eines Kampfjets (ca. 23 Mio. Zeilen Code). Die Erfahrung u.a. aus dem Betriebssystemumfeld zeigt, dass regelmäßig funktionale und sicherheitsrelevante Änderungen vorgenommen werden müssen. Zu klären ist, welche besonderen QS-Maßnahmen die Automobilindustrie diesbzgl. einrichten und wie ein LifeCycle hinsichtlich Gewährleistung, Garantie und Support geregelt wird. Wird es ein definiertes Ende des Supports für Software-Updates geben (vgl. Server- und Desktop-Betriebssysteme) und wie werden diese Updates bereitgestellt (automatisch, unbemerkt, kostenlos)?
- **Lebenszyklen, Updateregelungen und Gewährleistung bei hochautomatisierten Pilotierungssystemen:** Die Komplexität der Steuer- und Kommunikationssoftware wird es nötig machen, auch nach Auslieferung eines Fahrzeugs Anpassungen an den Programmen durchzuführen. Vollkommen ungeklärt ist derzeit die rechtliche Situation hinsichtlich der Produktlebenszyklen. Wird der Hersteller verpflichtet, „lebenslang“ und kostenfrei Updates für die sicherheitsrelevante Steuerungssoftware zu liefern, kann er den Support (vgl. Microsoft) nach X Jahren einstellen bzw. kostenpflichtig anbieten. Welche Erwartungen können an die Haltbarkeit elektronischer Bauelemente im Fahrzeug gesetzt werden (vgl. Alterung von Bauteilen)?
- **Code of Conduct für den Zugriff auf im Kfz gespeicherte Daten:** Als ein Ergebnis der Forschung soll ein Verhaltenskodex entwickelt und zur allgemeinen Verwendung vorgeschlagen werden, wer wann mit welcher notwendigen Legitimation auf im Kfz oder Smartphone gespeicherte Daten zugreifen darf und wie Hersteller einem Ermittler/Gutachter den Zugriff ermöglichen müssen.
- **Code of Conduct für den sicheren und vollständig anonymisierten Austausch von Geo-Daten:** Für den sicheren und vollständig anonymisierten Austausch von Daten (hier insbesondere Geo-basierte personenbezogene Daten) soll eine Handlungsempfehlung erstellt werden, wie dies unter technischen und datenschutzrechtlichen Aspekten rechtskonform und effektiv realisiert werden kann.
- **Datenlogger im Rahmen von Bonusprogrammen bei Kfz-Versicherern:** Einige Kfz-Versicherer bieten bereits Datenlogger für das Kfz an, bei denen der Fahrstil mit Bonus- und Malus-Punkten bewertet wird und anhand dessen sich die Versicherungsprämie bemisst. Unklar ist, ob und unterstellt wird, dass die Versicherer solche Datenlogger auch im Rahmen von Unfalluntersuchungen auslesen können und der Versicherte bei eigenem Fehlverhalten Nachteile in Kauf nehmen muss, die ihm ohne ein solches Gerät nicht nachgewiesen werden könnten.

- **Car-Sharing:** Gerade urbane Metropolen leiden erheblich unter dem zunehmenden Individualverkehr und u.a. seitens der Automobilindustrie werden deshalb Car-Sharing und Mobilitätsprojekte (incl. Elektromobilität) initiiert und ausgebaut. Diese fußen u.a. darauf, dass der Zugang zu den Fahrzeugen und die Abrechnung von Mietpreisen über Smartphones und IT-Infrastrukturen abgewickelt werden. Mobilitätskonzepte der Hersteller (z.B. Audi, Smart) sehen hierbei beispielsweise vor, den Benutzer über Portale der Hersteller zu vernetzen und ihm Zusatznutzen durch individualisierte Angebote bereitzustellen. Neben Fragen zur IT-Sicherheit (Zugang zu den Fahrzeugen, Missbrauch von Zugangsdaten) ist die Vernetzung unter Aspekten des Datenschutzes kritisch zu betrachten. Es lassen sich auf diese Weise Bewegungs- und Nutzungsprofile der Nutzer erstellen. Da die Anbieter zum Eigenschutz und zur Standortverwaltung ihre Fahrzeuge mit GPS überwachen, ist der jeweilige Nutzer zumindest für die Zeit der Benutzung lokalisierbar.
- **Geo-basiertes Advertising**: Die Automobilindustrie arbeitet an Konzepten, Geo-basierte Werbung und Informationen auf die Displays der Fahrzeuge zu übertragen (vgl. Vision von Audi im Rahmen des AMS-Kongress am 10.04.2014 in Stuttgart). Die rechtliche Zulässigkeit ist ungeklärt bzw. welche Rechtsnormen geschaffen werden müssten, um dies in Hinblick auf die Verkehrssicherheit und den Datenschutz zu realisieren.

4 Kooperationen

Der Autor ist an Kontakten und Kooperationen zur bzw. mit der Automobilindustrie, Zuliefern und Behörden sehr interessiert, um die Forschungsarbeit auf einer möglichst breiten und objektiven Basis aufzubauen.

Der gedankliche Austausch und die Diskussion ist hierbei genauso willkommen, wie konkrete Zusammenarbeit auf (daten-) technischem Niveau. Da die ersten Untersuchungen bereits sicherheitskritische Erkenntnisse geliefert haben, wird Projektpartnern ein entsprechend sensibler Umgang mit entsprechendem Wissen und Know-How zugesichert. Die Information der betroffenen Unternehmen über gefundene Sicherheitslücken vor einer angemessenen Veröffentlichung entspricht hierbei der üblichen Ethik unter Sicherheitsfachleuten.

Über Details von gemeinsamen Forschungsthemen können ggf. abgestufte Verschwiegenheitsklauseln vereinbart werden.

Direkte Projektpartner:

- Hochschule Albstadt Sigmaringen – Masterstudiengang Digitale Forensik
- Friedrich-Alexander-Universität Erlangen – Lehrstuhl technische Informatik - Prof. Freiling
- Ludwig-Maximilians-Universität München – Lehrstuhl Prof Vogel† (jetzt Lehrbeauftragter Dominik Brodowski)
- Fachhochschule Aachen – Prof. Hillgärtner / Prof. Schuba

5 Stand der Wissenschaft und Technik

Die Automobilindustrie ist derzeit vor allem damit beschäftigt, die neuen Technologien und Kommunikationskonzepte technisch und organisatorisch zu implementieren. Auf das Thema Sicherheit und Datenschutz und die nachfolgende forensische Auswertung von im Kfz-Umfeld gespeicherten Daten wird möglicherweise zurzeit wenig oder gar kein Schwerpunkt gelegt. Umso schwieriger und aufwändiger wird es nachher sein, Anforderungen der IT-Sicherheit umzusetzen, wenn die konzeptionelle Weichenstellung nicht frühzeitig im Entwicklungsprozess erfolgt. Gleichzeitig sinkt die Akzeptanz von Fahrerassistenzsystemen bei den Benutzern, wenn nicht transparent gemacht wird, welche Daten wo gespeichert werden und wer nachher darauf Zugriff hat. Es ist zudem zu erwarten, dass Kriminelle frühzeitig versuchen werden, die Systeme für ihre Zwecke zu missbrauchen, da hier ein erhebliches Potential für gewerblichen Betrug und Diebstahl zu erwarten ist. Gleichwohl werden Justiz und Ermittlungsbehörden die Anforderung stellen, auf diese Daten zuzugreifen bzw. Sachverständige werden von diesen Institutionen den Auftrag erhalten, entsprechende Daten zu beschaffen. Weder die Rechtslage noch die Art und Weise, wie dies angesichts der Komplexität und Vielfalt der Systeme technisch realisiert werden soll, sind derzeit im Rahmen eines unabhängigen Forschungsberichtes geklärt.

6 Marktumfeld und wissenschaftliche Konkurrenzsituation

Die Erkenntnisse aus der Forschungsarbeit werden im Rahmen eines öffentlich zugänglichen Berichtes allen Beteiligten und Interessierten zur Verfügung gestellt. Selbstverständlich wird es auch Bereiche geben, in denen aus Gründen der betrieblichen Geheimhaltung der Kreis der Adressaten eingeschränkt werden muss. Hiervon soll aber sehr gut überlegt und dosiert und nur im Ausnahmefall Gebrauch gemacht werden, wenn höhere Interessen überwiegen (z.B. bei Erkenntnissen über sicherheitskritische Schwachstellen, die nicht publik gemacht werden sollen, bevor diese geschlossen sind). Für die unmittelbar am Projekt beteiligten Personen, Unternehmen und Institutionen soll sich neben dem Erkenntnisgewinn natürlich auch ein Potential zur wirtschaftlichen Verwertung ergeben.

7 Über den Autor

Das Projekt wird von Dipl.-Ing. Thomas Käfer im Rahmen des berufsbegleitenden Masterstudiengangs Digitale Forensik an der Hochschule Albstadt-Sigmaringen initiiert, koordiniert und durchgeführt.

Dipl.-Ing. Thomas Käfer ist mit seinem IT-Systemhaus Käfer EDV Systeme GmbH seit 1990 selbstständig in der IT tätig (5 Mitarbeiter). Er arbeitet seit 2002 als Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung (seit 2006 öffentlich bestellt), als IT-Consultant, Fachautor und Dozent für die IT-Spezialistenausbildung und beschäftigt sich vor allem mit Fragen der IT-Sicherheit, dem Datenschutz und dem Gebiet der Digitalen Forensik. Ehrenämter als Handelsrichter am Landgericht Aachen, IHK-Prüfer für Auszubildende im Bereich Fachinformatik und Weiterbildungsmaßnahmen als IT-Projektleiter sowie als Mitglied der Vollversammlung der IHK Aachen runden die Aktivitäten ab.


Digitale Kfz-Forensik
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung,
eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung


Car-Forensics
Dipl-Ing. Thomas Käfer
www.KaeferLive.de
Forschungsarbeit / Masterthesis Digitale Kfz Forensik
Digitale Kfz-Forensik
www.car-forensics.de
Dipl-Ing. Thomas Käfer
Critical
Safety
Updateregelungen
Unfalldatenschreiber
CAN
Navigationsgeräte
Hardware
Car2Phone
Conduct
Security
Fahren
Piloted
Logging
Car2Car
Software
Notruf-Systeme
Angriffsvektoren
Pen-Tests
Automotiv
Bus
Missbrauchsszenarien
Automatisches
Datenschutz
Autonomes
App
Steuergeräte
Datenlogger
Lebenszyklen
of
Gewährleistung
Automotiv-Smartphone-Apps
Car2X
Angriffsszenarien
Qualitätssicherung
und
Pay-As-You-Drive
Betriebssicherheit
für
Code
Angriffsflächen
eCall
Geodaten
Car2Person
Haftungsfragen
2


Car-Forensics
Dipl-Ing. Thomas Käfer
www.KaeferLive.de
Aspekte und Themenfelder der Forschungsarbeit
Angriffsszenarien für Automotiv-Smartphone-Apps
Betriebssicherheit von Kfz (Safety Critical) und IT-Sicherheit (Security Critical) bei Kfz/Car2X
Datenschutz- und Datensicherheitsaspekte bei Car2X-Kommunikation und -Infrastrukturen
Unfalldatenschreiber (Technik, Zugriffsregeln, Datenschutz, Validität, Nemo tenetur-Grundsatz)
Automatisches Notruf-Systeme eCall (Datenschutz, Profilerstellung, Ortungsmöglichkeit)
Haftungsfragen und Datenschutz beim automatisierten Pilotieren von Kfz
Notwendige Rechtsreformen für automatisiertes Pilotieren von Kfz
Forensische Auswertungsmöglichkeiten von Logs von Navigations- und Steuerungsgeräten
ZIELE
3

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

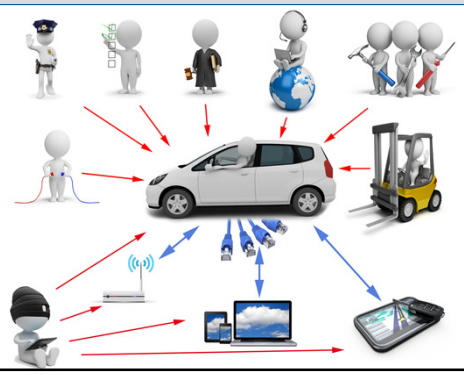
Fragestellungen der Forschungsarbeit

- Was wird digital wo in welchem Umfang wie für wie lange gespeichert?
- Wer hat Zugriff auf die Daten?
- Wem „gehören" die Daten?
- Wie sicher sind die Daten / Systeme?
- Was davon sind personenbezogene Daten und unterliegen damit dem Datenschutz?
- Was lässt sich forensisch wie und von wem auswerten?
- Was lässt sich für kriminelle Zwecke missbrauchen?
- Welche gesetzlichen Rahmenbedingungen gibt es und welche müssen neu geschaffen werden?

4

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Schnittstellen und Akteure definieren die Angriffsflächen und die Angriffsvektoren



5

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Missbrauchs- und Angriffsszenarien: Past – Present – Future

- Fahrzeug ohne Fahrerassistenzsysteme
- keine digitalen Systeme
- keine digitalen Schnittstellen
- keine externe Vernetzung

6


Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de
Missbrauchs- und Angriffsszenarien: Past – Present – Future
Fahrzeug ohne Fahrerassistenzsysteme
keine digitalen Schnittstellen
nur interne/ keine externe Vernetzung
7


Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de
Missbrauchs- und Angriffsszenarien: Past – Present – Future
Fahrzeug mit Fahrerassistenzsystemen – teilautonomes Fahren
viele digitale Schnittstellen
umfangreiche interne und externe Vernetzung
8


Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de
Missbrauchs- und Angriffsszenarien: Past – Present – Future
Autonom fahrende und voll vernetzte Fahrzeuge
P
HH UY 1082
9

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Missbrauchs- und Angriffsszenarien: Past – Present – Future

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

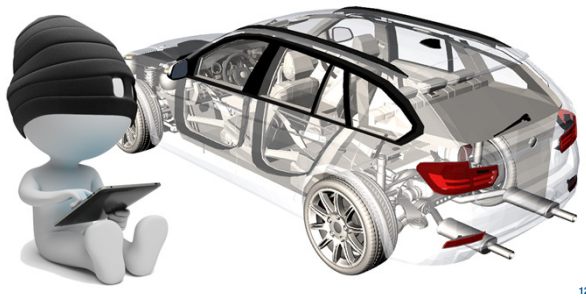
Missbrauchs- und Angriffsszenarien

- SPAM auf den PC ist nervig.
- Phishing auf dem PC ist ärgerlich.
- Online-Banking-Betrug ist kostspielig.
- Angriffe auf Fahrzeuge sind in letzter Konsequenz tödlich.

11

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Erste Forschungsergebnisse: Angriffsszenarien auf Automotiv-Apps

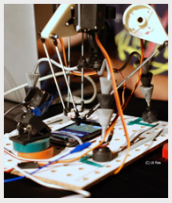


12

Car-Forensics | Dipl-Ing. Thomas Käfer | Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung | www.KaeferLive.de

Erste Forschungsergebnisse - Unsicherheit von Automotiv-Apps

- Konkrete Funde in der APP BMW Remote (ConnectedDrive):
  - PIN der App: „1234" im Klartext in der Apple Keychain gespeichert
  - AES Schlüssel-Datenbank: 1INdeJ7ktzzhzGQucH2uX0zPkEvI8K4n (im Klartext in der Apple Keychain gespeichert)
  - VIN: xxxxxx
  - Kennzeichen: AC-I.....
  - Benutzername: Thomas.TK.Kaefer
  - Benutzer ID 678xxx im Automotiv-Portal
  - Passwort: Bananen1234. -> „codiert" als FBD8D7D8D7DCD7888B8A8D97 (X-OR mit B9)
  - Alle Ausstattungscodes des Fahrzeugs
  - Farbe des Fahrzeugs
  - Aktueller Standort (GPS-Peilung)
  - Zugriff auf Lichthupe, Hupe, Klimaanlage und Türöffner

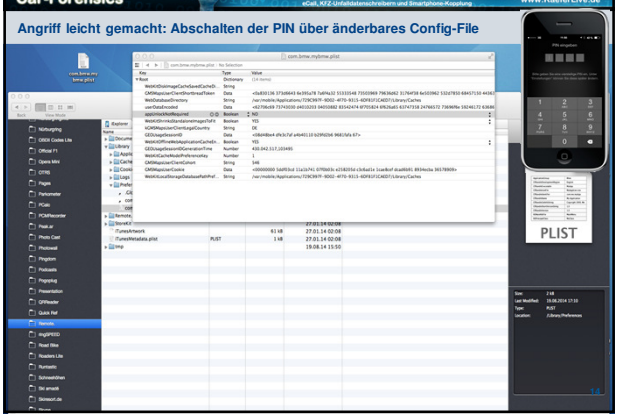


- 4-Stelliger Passcode-Schutz des iPhone ist in max. 17 Stunden automatisiert zu brechen (wenn Benutzer nicht die Option „Daten löschen nach 10 Versuchen" aktiviert hat).

13

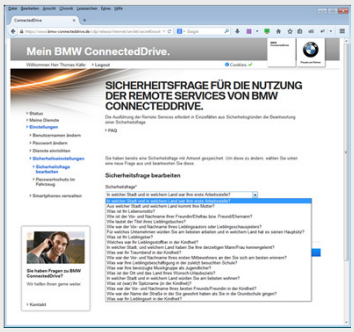
Car-Forensics | Dipl-Ing. Thomas Käfer | Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung | www.KaeferLive.de

Angriff leicht gemacht: Abschalten der PIN über änderbares Config-File



Car-Forensics | Dipl-Ing. Thomas Käfer | Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung | www.KaeferLive.de

Angriff durch Social Engineering leicht gemacht: Trivialität von Sicherheitsfragen



15

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Angriff leicht gemacht: Unverschlüsselte Datenablage

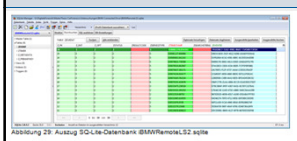
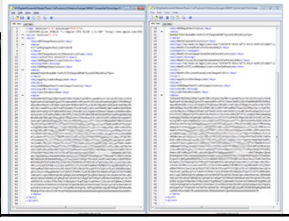


Abbildung 29: Auszug SQLite-Datenbank iBMWRemoteLS2.sqlite

Die Daten in der PList-Datei sind also offensichtlich nicht verschlüsselt, sondern nur als Hexadezimalwerte abgelegt. Man erhält auf diese Weise aus der vollkommen unverschlüsselten PList-Datei ohne Jailbreak allein mit dem Export der Datei mittels iExplorer mindestens folgende Daten:

- Benutzername
- VIN
- Kennzeichen
- Datum der Erstzulassung
- Modell
- Farbe

Ein weiterer Nachweis, dass diese Daten nicht mit einem gerätespezifischen Schlüssel chiffriert worden sind, ergibt sich, wenn man die gleichen Daten auf zwei verschiedenen iPhones eingibt und anschließend die PList-Dateien vergleicht. Der komplette Bereich „User Data Encode" ist identisch (Beweis These 11).



Hierbei entspricht das Feld „ZTIMESTAMP" dem Datum und der Uhrzeit der Aktion im Mach-Format*. Mittels im Internet verfügbarer Tools** gelingt die Umrechnung beispielsweise von „430861370.054361" in „18.08.2014 21:02:50 Uhr". Durch Abgleich mit den in der App angezeigten Daten gelingt der Rückschluss der Bedeutung von „ZSERVICETYPE" auf einfache Weise.

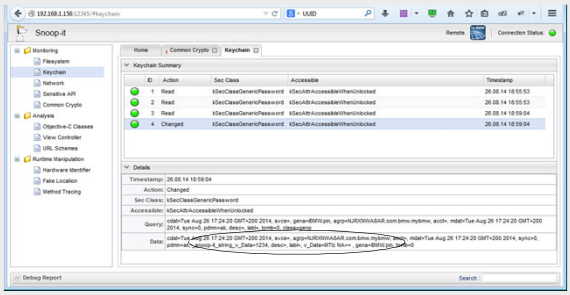
Hierbei entsprechen die Werte ZSERVICETYPE fo

ZSERVICETYPE	Dienst
5	Lichthupe
4	Hupe
3	Türentriegelung
2	Türverriegelung
1	Fahrzeuglokalisierung

* Mach-Format: Numerisches Format für die Absolut-Zeit, typ
** z.B. http://www.gaijin.at/dlutils.php

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

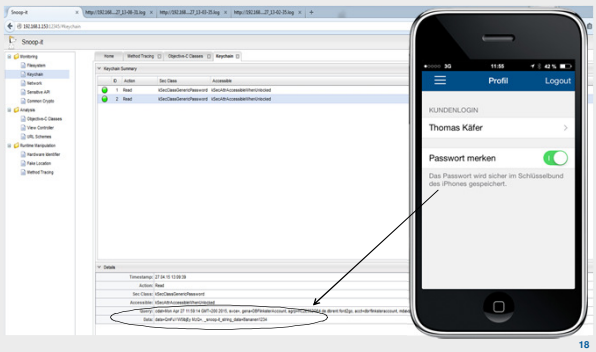
PIN auslesen leicht gemacht: Beispiel BMW



17

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Passwort auslesen leicht gemacht: Beispiel Ford Car-Sharing (DB-Rent / Flinkster)



18

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Die Apple-Keychain ist sicher… (frei nach Norbert Blüm: Die Rente ist sicher…)

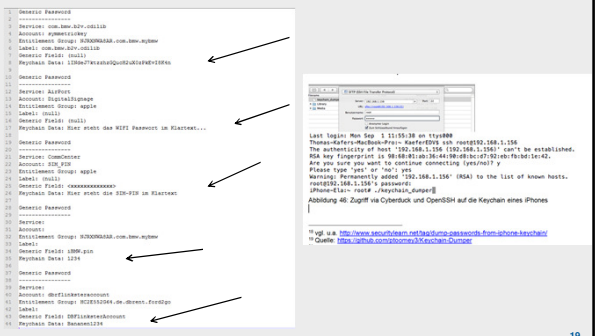


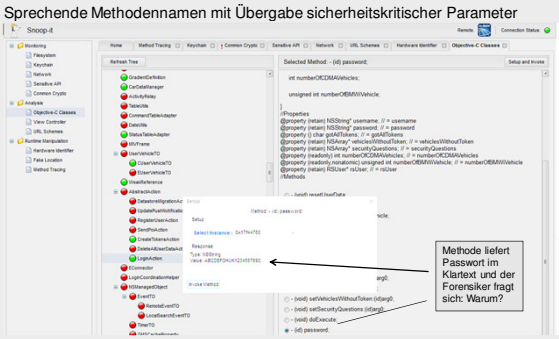
Abbildung 46: Zugriff via Cyberduck und OpenSSH auf die Keychain eines iPhones

[1] vgl. u.a. http://www.securitylearn.net/tag/dump-passwords-from-iphone-keychain/
[2] Quelle: https://github.com/ptoomey3/Keychain-Dumper

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Analyse mit Snoop-it und einem Keychain-Dumper nach Pangu-Jailbreak

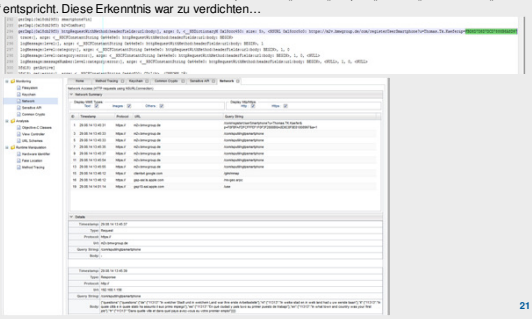
Sprechende Methodennamen mit Übergabe sicherheitskritischer Parameter



Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

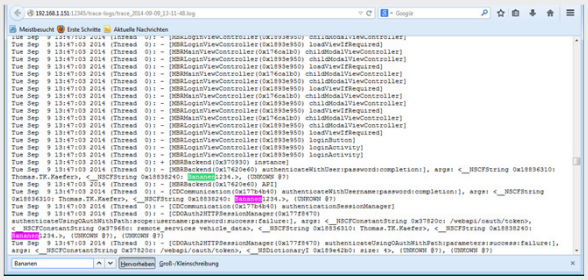
Fundstellen Passwort (XOR-codiert)

Hierbei lautet das Klartext-Passwort „Bananen1234.". Dies entspricht dem Cipher-Text „FBD8D7D8D7DCD7888B8A8D97". Man erkennt z.B., dass die „1" der „88", die „2" dem „8B" und das „n" dem „D7" entspricht. Diese Erkenntnis war zu verdichten…



Car-Forensics — Dipl-Ing. Thomas Käfer — Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung — www.KaeferLive.de

Unverschlüsselte Verarbeitung des Benutzerpasswortes (V 3.0)



22

Car-Forensics — Dipl-Ing. Thomas Käfer — Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung — www.KaeferLive.de

Fundstellen Passwort (XOR-codiert)

Mit drei systematischen Passwortänderungen über den gesamten Buchstaben- und Zahlenbereich im Portal und dem anschließenden Auslesen des Cipher-Codes erhält man dann das praktisch vollständig entschlüsselte Cipher-Alphabet:

```
A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
F8 FB FA FD FC FF FE F1 F0 F3 F2 F5 F4 F7 F6 E9 E8 EB EA ED EC EF EE E1 E0 E3

a  b  c  d  e  f  g  h  i  j  k  l  m  n  o  p  q  r  s  t  u  v  w  x  y  z
D8 DB DA DD DC DF DE D1 D0 D3 D2 D5 D4 D7 D6 C9 C8 CB CA CD CC CF CE C1 C0 C3

1  2  3  4  5  6  7  8  9  10 .
88 8B 8A 8D 8C 8F 8E 81 80 B9 97
```

Man erkennt mit ein wenig kryptografischen Verständnis, dass es sich hierbei um eine XOR-Verschlüsselung mit dem Schlüssel B9 handelt. Den Schlüssel findet man (wenn nicht durch Ausprobieren) durch Analyse der Methodenaufrufe (Beweis These 8):

RSCryptoUtils(0x37f0d8) cipherString:withMask:], args: <__NSCFString 0x1947b440: ABCDEFGHIJK1234567890.>, <__NSCFString 0x169b3750: B9>

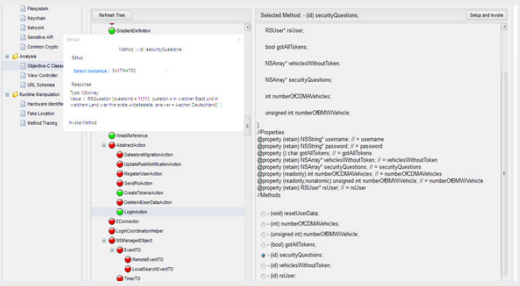
https://m2v.xxx.de/com/registerUserSmartphone?u=Thomas.TK.Kaefer&p=D8DBDADDDCDFDED1D0D3D2D5D4D7D6C9C8CBCACDCCCFCEC1C0C38897&a=1

23

Car-Forensics — Dipl-Ing. Thomas Käfer — Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung — www.KaeferLive.de

Antworten auf die Sicherheitsfrage (V 2.8) liegen im Klartext vor (ohne Hash)

Die Sicherheitsfrage und die passende Antwort kann man mit Snoop-IT und dem Aufruf der Methode „answer“ aus der Klasse „RSQuestion“ ebenfalls ermitteln:



24

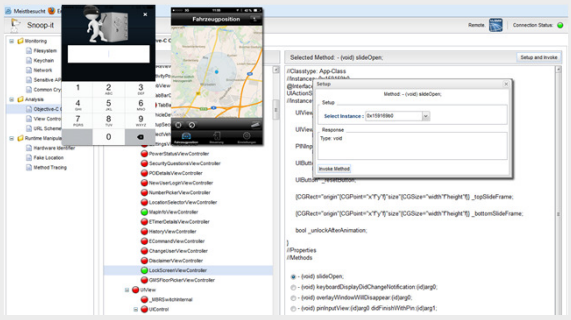
Car-Forensics

Dipl-Ing. Thomas Käfer

Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung

www.KaeferLive.de

Überspringen des Sperrbildschirms mittels Methodenaufruf in Snoop-it



25

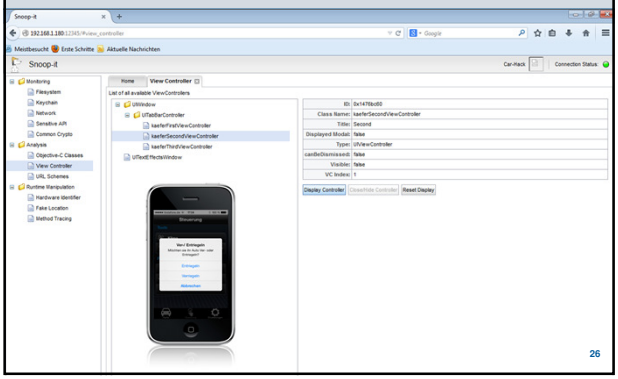
Car-Forensics

Dipl-Ing. Thomas Käfer

Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung

www.KaeferLive.de

Simpler Nachbau – Schwachstelle praktisch aller Apps, die diesem Design folgen…



26

Car-Forensics

Dipl-Ing. Thomas Käfer

Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung

www.KaeferLive.de

Neuer Fehler in Version 3.0 – Ändern der PIN im Sperrbildschirm der APP

Die PIN lautet hier zu Beginn des Vorgangs „2004".

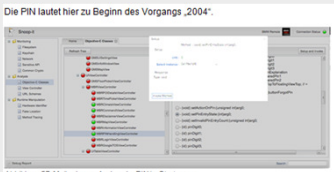
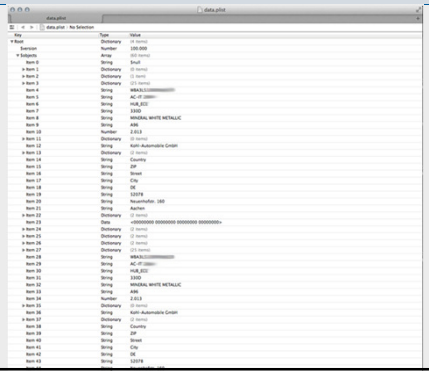


Abbildung 57: Methode zum Ändern der PIN im Startscreen

Dann erfolgt der Aufruf der Methode „setPinEntryState" der Klasse „MBRPINHandlingViewController" mit dem Übergabewert „0"

27

Unverschlüsselte Ablage der Daten in der PList-Datei – Zugriff ohne Jailbreak möglich



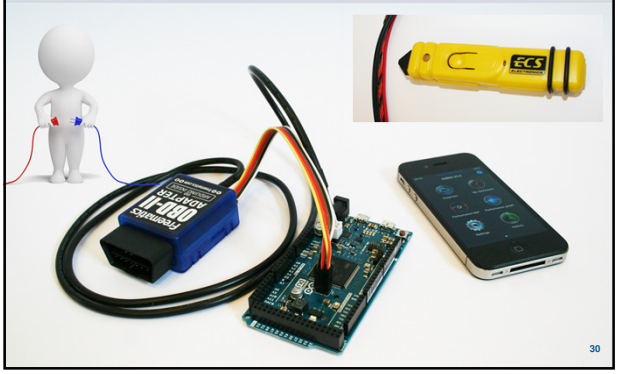
28

Verbesserungen und Verschlechterungen in einer untersuchten App

- **Verbesserungen in Version 3.0 im Vergleich zu Version 2.8 :**
  - Die PIN-Abfrage kann nicht mehr allein durch Änderung der PList-Datei abgeschaltet werden, da zusätzlich ein Indikator (Boolescher Wert true/false) in der Apple-Keychain gespeichert wird.
  - Es existiert keine SQLite-Datenbank mehr, in der die Fahrzeugdaten abgelegt sind. Hierdurch reduziert sich die Angriffsfläche.
  - Der Viewcontroller zur Steuerung der Fahrzeugfunktionen Hupe, Lichthupe und dem Öffnen der Türen ist ohne korrekte PIN-Eingabe nicht via Jailbreak/Snoop-IT anwählbar (wenngleich diese Funktionen immer noch über die Methodenaufrufe möglich sind).
  - Durch Wegfall der SQLite-Datenbank wird ein Teil der benutzer- und fahrzeugspezifischen Daten nicht mehr über den Zeitpunkt des Löschens der App vom Endgerät hinaus gespeichert.
- **Verschlechterungen in Version 3.0 im Vergleich zu Version 2.8**
  - Im File „data.plist" kann man den Namen des zuständigen BMW-Händlers im Klartext incl. Adressinformationen auslesen. Diese Informationen kann man im Rahmen des Social Engineerings nutzen und deren Speicherung in der App ist im Übrigen aus Datenschutzsicht nicht unbedenklich. Fraglich ist, warum diese Information überhaupt in der App gespeichert ist, da sie über deren Oberfläche gar nicht abgerufen werden kann.
  - Die PIN kann mittels Jailbreak/Snoop-IT im Viewcontroller/Screen der PIN-Abfrage selbst ohne Kenntnis selbiger durch einen Angreifer geändert werden.
- **Wesentliche Mängel sind in der aktuellen Version 3.1.3 vom 30.03.2015 nach rd. einem halben Jahr seitens BMW immer noch nicht gefixt.**

29

Erste Forschungsergebnisse: Angriffsszenarien auf Fahrzeug-Bus-Systeme



30


Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de
Bussysteme und Schnittstellen im Kfz – Wunsch und Wirklichkeit
OBD-Schnittstelle
ZIELE
Firewall / Gateway
Fahrzeugbusse (CAN, MOST, Ethernet, Flex u.a.)
Steuergerät
Steuergerät
Steuergerät
Steuergerät
31

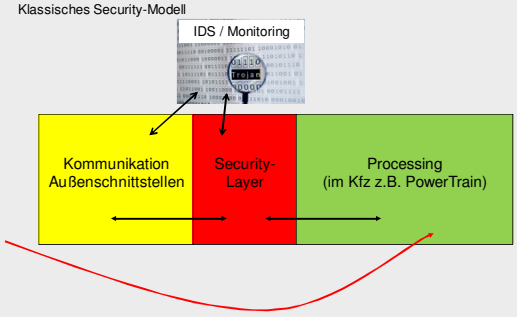

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de
Missbrauchs- und Angriffsszenarien: Reifendrucksensoren - Tracking und Spoofing


Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de
Missbrauchs- und Angriffsszenarien
Manipulation von Bus-Signalen (GPS, Steuerwertdaten)
Ohne Verschlüsselung haben Hacker leichtes Spiel…
Gegenmaßnahmen: u.a. Validierung, Verschlüsselung, Hashing, Intrusion Detection, Firewall und Forensic Readyness
YOUR CAR HAS BEEN HACKED!
300 KM/H
33

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Warum funktionieren solche Angriffe?

- Klassisches Security-Modell

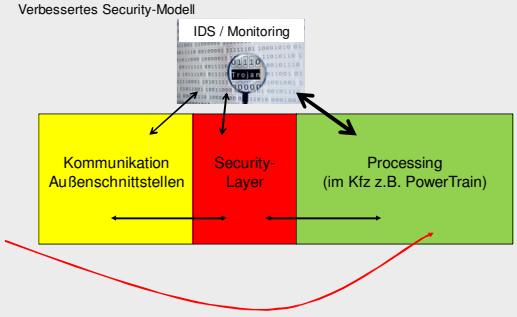


34

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Warum funktionieren solche Angriffe?

- Verbessertes Security-Modell



35

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Problemstellungen für die Forensik und sicherheitsrelevante Auswirkungen

- Für den Forensiker: Ohne genormte Datenschnittstellen und digitale Speicher ist eine Rekonstruierung eines Tat- oder Unfallhergangs (bei einem autonom fahrenden Fahrzeug) nicht oder nur mit Hilfe des Automobil-Herstellers oder Zulieferers möglich.
  - Hersteller will Wissen nicht an Dritte herausgeben
  - Hersteller kennt zugekaufte Steuergeräte im Detail ggf. gar nicht ausreichend gut
  - Hersteller ist jedoch bei einem Zivil- oder Strafverfahren Beteiligter oder Beschuldigter
  - Konsequenz: Hersteller will oder braucht nicht an der Aufklärung mitwirken bzw. wird nur dann kooperativ sein, wenn es zu seiner Entlastung beiträgt (nemo tenetur). In Zivilstreitigkeiten (Produkthaftung) ist sein Mitwirken ein Parteivortrag und damit weniger glaubwürdig, als ein von einem unabhängigen Sachverständiger erstelltes Gutachten.

36

Verschlüsselung

Car-Forensics

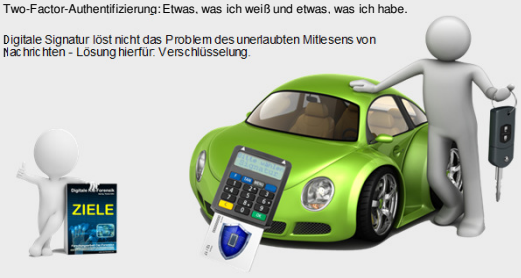
Dipl-Ing. Thomas Käfer

Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung

www.KaeferLive.de

Gegenmaßnahmen: Digitale Zertifikate, Digitales Signieren und Verschlüsselung

- Digitale Zertifikate / Signaturen zur Authentifizierung / Validierung nutzen.
- Ziel: Identifikation des Absenders einer Nachricht bzw. des Nutzers bei einem Login – Überprüfung, ob eine Nachricht authentisch ist.
- Anonymisierte und nicht-anonyme Authentifizierung realisierbar und sinnvoll (Datenschutz).
- Two-Factor-Authentifizierung: Etwas, was ich weiß und etwas, was ich habe.
- Digitale Signatur löst nicht das Problem des unerlaubten Mitlesens von Nachrichten - Lösung hierfür: Verschlüsselung.



37

Falltür-Algorithmus

Car-Forensics

Dipl-Ing. Thomas Käfer

Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung

www.KaeferLive.de

Gegenmaßnahmen: Digitale Hashes anstelle von Klartext-Passwörtern

- Berechnung funktioniert einfach in die Verschlüsselungs- bzw. Kodierungsrichtung.
- Berechnung in Entschlüsselungsrichtung ist sehr aufwändig bis unmöglich.
- Man spricht daher von einem Falltür-Algorithmus.
- Solche Verfahren sind i.d.R. nur durch Brute-Force-Attacken zu knacken, d.h. durch maschinelles Ausprobieren.
- Vergleich der Hashes (des Hackfleisches), nicht der Klartexte (Schweine).
- Standardverfahren: mindestens MD5, oder SHA 1 – besser SHA 256 oder SHA 512.

38

Car-Forensics

Dipl-Ing. Thomas Käfer

Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung

www.KaeferLive.de

Gegenmaßnahmen: Denken wie die Hacker

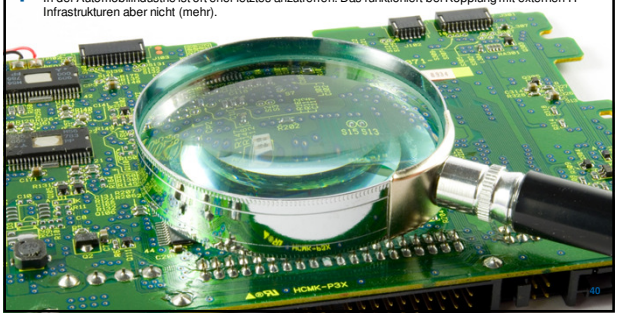
- Denken Sie wie die Hacker und seien Sie kreativ: In jeder guten Anwendung steckt auch eine dunkle Seite (vgl. Autopilot bei Schiffen und deren Missbrauch bei führerlosen Flüchtlingsfrachtern im Mittelmeer).
- White-Box- und Entwicklertests sind gut – Man braucht aber auch externe Blackbox-Tests!
- Externe Pen-Tester (Sicherheitsfachleute / Forensiker) suchen systematisch nach Schwachstellen (so wie die Hacker).

39

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Must Do: Beachtung des Kerckhoff'schen Prinzips (missachtet in der Automobilwelt)

- Kerckhoff'sches Prinzip: Sicherheit eines Systems soll auf der Geheimhaltung der Schlüssel und nicht des Algorithmus beruhen (im Gegensatz zu „Security through obscurity").
- In der Automobilindustrie ist oft eher letztes anzutreffen. Das funktioniert bei Kopplung mit externen IT-Infrastrukturen aber nicht (mehr).



40

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

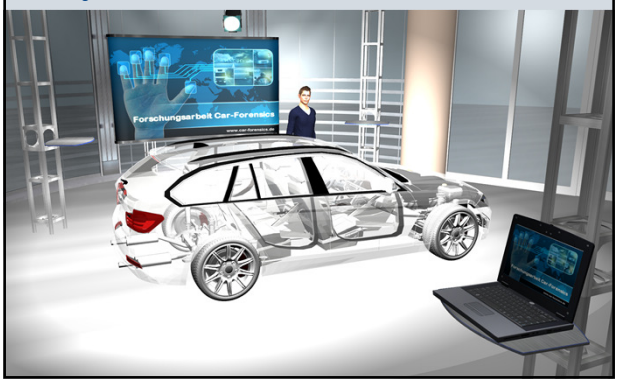
Sicherheit = Produktqualität

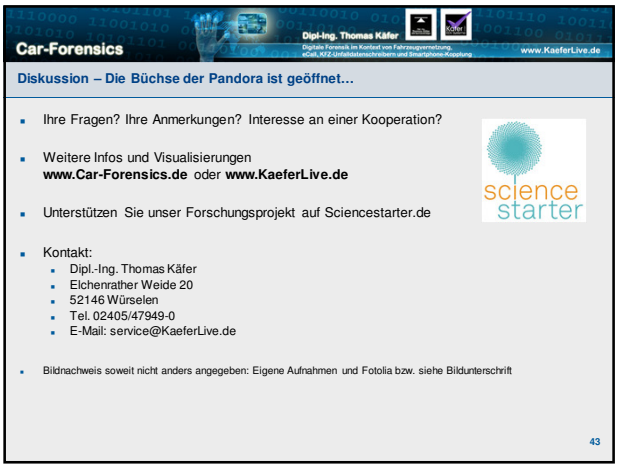
- 2014 erreichten die weltweiten Rückrufe der Automobilhersteller einen neuen Negativ-Rekordstand. Wie will die Autoindustrie bei wachsender Komplexität diesen Qualitätsproblemen begegnen?
- Welche Vorgaben macht der Gesetzgeber bzgl. Gewährleistung, LifeCycle und Updategarantien?

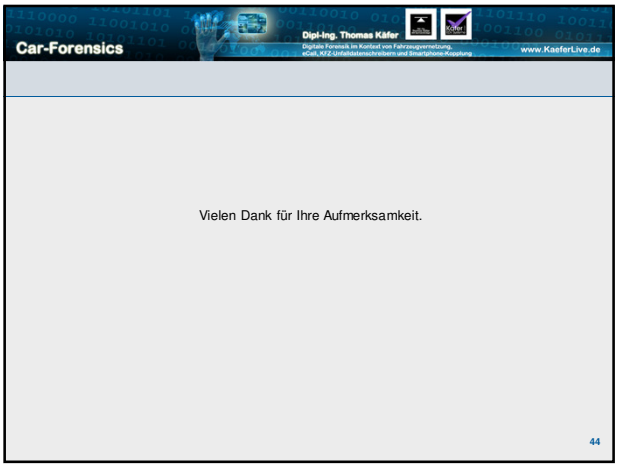
41

Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de

Interesse geweckt?




Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de
Diskussion – Die Büchse der Pandora ist geöffnet...
Ihre Fragen? Ihre Anmerkungen? Interesse an einer Kooperation?
Weitere Infos und Visualisierungen
www.Car-Forensics.de oder www.KaeferLive.de
Unterstützen Sie unser Forschungsprojekt auf Sciencestarter.de
science starter
Kontakt:
Dipl.-Ing. Thomas Käfer
Elchenrather Weide 20
52146 Würselen
Tel. 02405/47949-0
E-Mail: service@KaeferLive.de
Bildnachweis soweit nicht anders angegeben: Eigene Aufnahmen und Fotolia bzw. siehe Bildunterschrift
43


Car-Forensics
Dipl-Ing. Thomas Käfer
Digitale Forensik im Kontext von Fahrzeugvernetzung, eCall, KFZ-Unfalldatenschreibern und Smartphone-Kopplung
www.KaeferLive.de
Vielen Dank für Ihre Aufmerksamkeit.
44