The automobile as massive data gathering source and the consequences for individual privacy

31C3, 28.12.2014

Jimmy Schulz,
Chaos Computer Club
Wolfram Hell LMU

Spiegel online

AUDI

Modell: Audi A8 (2014)
Angriffsfläche für Hacker: ++
Netzwerk-Architektur: --
Gefahr bei Assistenzsystemen: +

Ein Plus (+) steht für "leicht zu hacken", ein Minus (-) für "weniger angriffsfähig".

Jeep

lodell: Jeep Cherokee (2014)
ngriffsfläche für Hacker: ++
letzwerk-Architektur: ++
efahr bei Assistenzsystemen: ++

Modell: BMW 3er (2014)
Angriffsfläche für Hacker: ++
Netzwerk-Architektur: --
Gefahr bei Assistenzsystemen: +

Ein Plus (+) steht für "leicht zu hacken", ein Minus (-) für "weniger angriffsfähig".

Modell: Toyota Prius (2014)
Angriffsfläche für Hacker: +
Netzwerk-Architektur: +
Gefahr bei Assistenzsystemen: ++

Ein Plus (+) steht für "leicht zu hacken", ein Minus (-) für "weniger angriffsfähig".

AP

Modell: Toyota Prius (2010)
Angriffsfläche für Hacker: +
Netzwerk-Architektur: +
Gefahr bei Assistenzsystemen: ++

Ein Plus (+) steht für "leicht zu hacken", ein Minus (-) für "weniger angriffsfähig".

Modell: Toyota Prius (2006)
Angriffsfläche für Hacker: -
Netzwerk-Architektur: --
Gefahr bei Assistenzsystemen: --

Ein Plus (+) steht für "leicht zu hacken", ein Minus (-) für "weniger angriffsfähig".

Spiegel online

Tesla Model S: Hacker-Attacke bei voller Fahrt

Tesla

Tesla Model S: Von Studenten fremdgesteuert

Chinesische Studenten haben ein Tesla Model S gehackt: Sie manipulierten ein fahrendes Auto und steuerten Türen und Schiebedach des Wagens fremd. Der Elektroautohersteller hat bereits auf den Angriff reagiert.

The automobile as massive data gathering source and the consequences for individual privacy

Agenda

Hacker OBD2
Google vs. OEM: Wem gehört Dein Auto?
Vorratsdatenspeicherung/Totalüberwachung

Hacker OBD2

Bis dato:
•Bluetooth
•„Sitting in the car“ und Stecker
•WiFi

Hacker OBD2
Welche Daten?

Technische Geräte:
ECU, OBD2, CAN-Bus, ...

Alle Daten,
-für die es Sensoren und Aktoren gibt
-in einer Granularität, Dauer und Form (z. B. Threshholds), die vom Memory abhängt.

Einfache Daten:
Geschwindigkeit, Tankstand, GPS-Koordinaten, Beschleunigung, Drehzahl, ...

Abgeleitete Daten:
Verbrauch, Durchschnittsgeschwindigkeit, Geschwindigkeitsüberschreitung

Andere Daten:
Funkzellen

Es gibt keine Eigentumsrecht an Daten!

Google vs. OEM: Wem gehört Dein Auto?

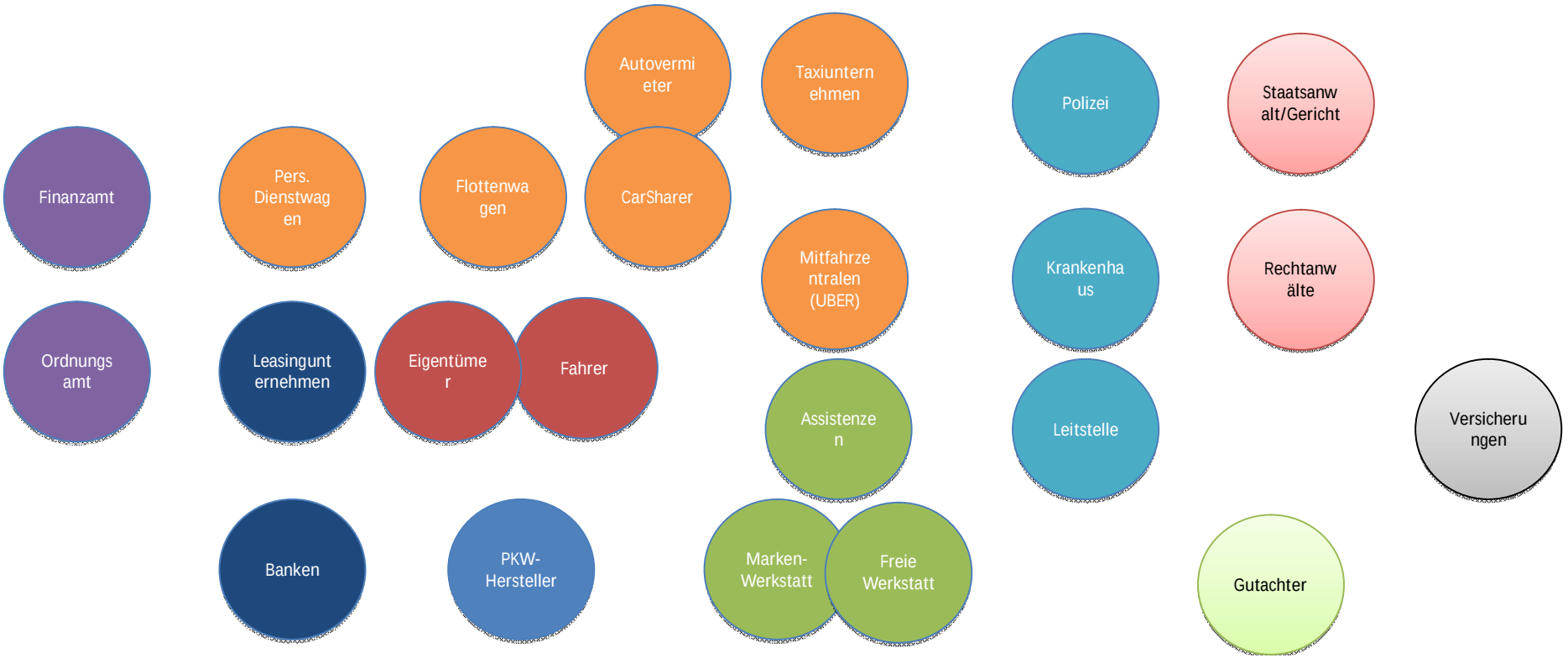
Winterkorn am 20. März 2014 anlässlich des 16. Technischen Kongresses des VDA in Hannover:

automobil-produktion.de: “Was wir nicht wollen, ist, dass diese Daten unserer Kunden irgendwo hinwandern.”
tagesschau.de: VW-Chef Winterkorn reklamierte den Besitzanspruch für all diese Informationen: "Die Daten gehören uns!“

Nach den VDA Prinzipien vom 10.11.2014 gibt es:
a)Fahrzeugbezogenen Daten (wie Kilometerstand)
b)Personenbezogene Daten (wie Anschrift)
c)Service relevante technische Daten aus der Klasse der Fahrzeugbezogenen Daten.
d)Personenbezogene Daten unterliegen der Hoheit des Fahrers, können aber zum Ausschluss von Servicen führen, wenn die Speicherung abgelehnt wird.
e)Assistenz- und Infotainment Daten, die zu löschen sind.

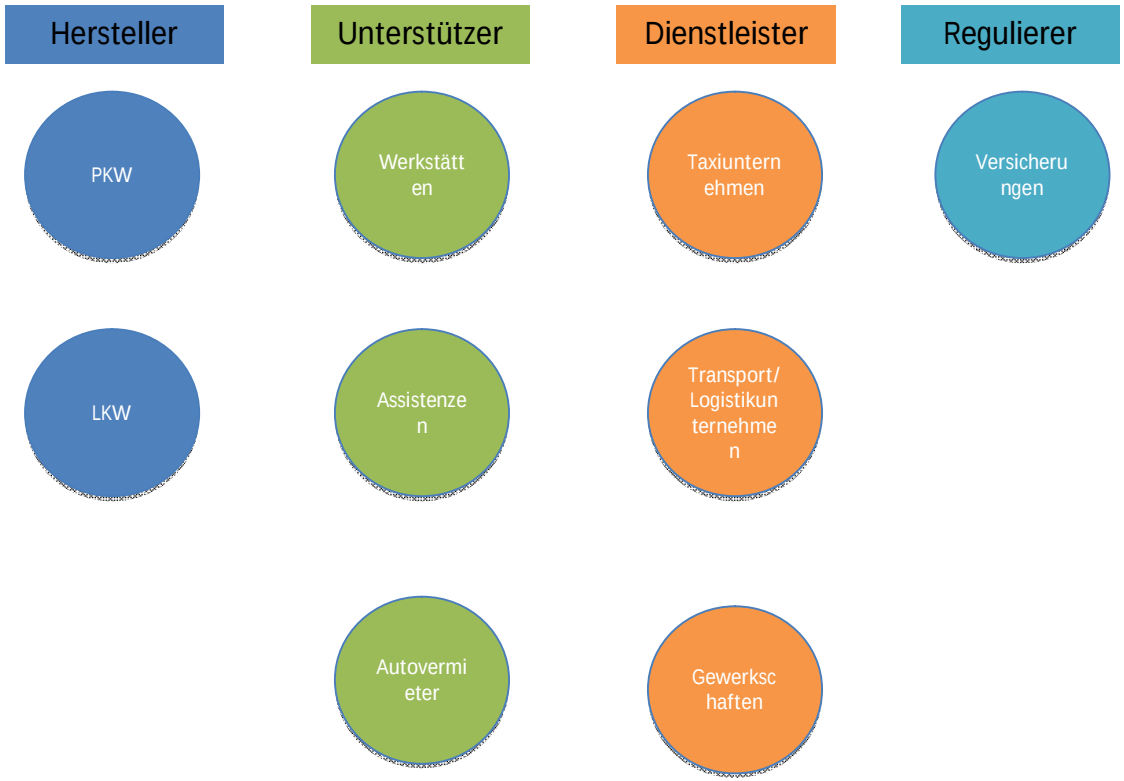
Wem gehört Dein Auto?

Beispiel PKW (unvollständig)



Wem gehört Dein Auto

Teilnehmer an der Umfrage



Vorratsdatenspeicherung/Totalüberwachung

Wo werden die Daten gespeichert?
a)Im Fahrzeug (teilweise in unbekannter Granularität und Dauer)
b)Im RZ eines OEM‘s (Nutzung von Onlinediensten oder Motorüberwachung oder Werkstattbesuch)
Tendenz der Cloud-Dienste (mehr, genauer, präziser, länger)
c)Bei Google, Microsoft, Apple,... im Rahmen der Smartphones oder der Apps im Fahrzeug.

Legaler Zugriff:
Zu a) Gefahr in Verzug und damit Vollzugriff: Staat (Polizei, Staatsanwaltschaft)
Zu b) Richterliche Anordnung: Staat (Polizei, Staatsanwaltschaft)
Zu c) Richterliche Anordnung: Staat (Polizei, Staatsanwaltschaft)

Angriffsvektoren:
Ad a): Geheimdienste, Kriminelle, Beziehungen
Ad b): Geheimdienste, Kriminelle
Ad c): Geheimdienste, Kriminelle

Befragung

Automobilhersteller: 8 (1)
Landmaschinen-Hersteller: 3

Werkstätten/Händler: 8 (1)

Assistenzen/Automobilclubs: 3

Autovermieter: 4 (1)

Spediteure 3 (2)

Logistiker: 2

Versicherungen: 4

Befragung

Gesamt: Angefragt: 40/Geantwortet: 17/Substantiell geantwortet: 9

Automobilhersteller: 9/5/2
Landmaschinen-Hersteller: 3/0/0

Werkstätten/Händler: 9/3/3

Assistenzen/Automobilclubs: 3/2/2

Autovermieter: 4/4/2

Spediteure: 6/1/0

Logistiker: 2/0/0

Versicherungen: 4/2/0

Assistenzen/Automobilclubs

Geschäftsmodell: Pannenhilfe/Fahrer wieder mobil machen (eher ältere Autos)

Aktivitäten: Kleinere Reparaturen vor Ort, Transport in die Werkstatt, Stellung von Ersatzwagen

Benötigte Daten: Motorsteuerdaten, Fehlerdaten, Datenänderungsrechte

Hinweis: Stellen teilweise auch die Mobilitätsgarantie für KFZ Hersteller zusammen mit Mietwagenunternehmen.

Werkstätten/Händler

Geschäftsmodell: Reparatur von Fahrzeugen, Wartung, Garantie

Aktivitäten: Reparaturen, Wartung, Garantie

Benötigte Daten: Motorsteuerdaten, Fehlerdaten, Herstellerdaten zum Fahrzeug, Datenänderungsrechte

Hinweis: KFZ Handwerk fordert „interoperable, standardisierte, sichere und frei zugängliche Plattform“ bei Typenzulassung auf Ebene EU; Wettbewerb zwischen freien und markengebundenen Werkstätten

Probleme

- Manche Hersteller sind sich Angriffsfläche nicht bewusst (z.B. auch keyless go)
- Zusätzliches Fehlerpotential das im Extremfall zu einem Unfall führen kann
- Dann Dokumantation/Beweis?
- (Teil)Autonomes Fahren dann problematisch
- Fahrzeughersteller steigen immer mehr z.B. auf Android also klassische Computersysteme um

Gmttb Forderungen

- EDR Speicherung relevanter Daten
- Offene OBD Schnittstellen zur Auslesung Fehlerspeicher
- Systemarchitektur nicht von außen drahtlos beeinflussbar
- Mehr Problembewußtsein und sichere Standards
- Regelmäßige Sicherheitsupdates vom Hersteller