# Sicheres Datenmanagement im Automobil: Eine Komponentenorientierte Sicht

Prof. Dr.-Ing. Jana Dittmann

AG Multimedia and Security
Institut für Technische und Betriebliche Informationssysteme (ITI)
Fakultät Informatik (FIN)
Otto-von-Guericke Universität Magdeburg

Europäische Kommission
Europäische Strukturfonds
INVESTITION IN IHRE ZUKUNFT

***Danksagungen:*** *Diese Veröffentlichung entstand in Kooperation mit dem Verbundprojekt COmpetence in MObility (COMO, EU-Nr.: C-2007-5254). Der Inhalt dieser Veröffentlichung steht in alleiniger Verantwortung der Autoren und widerspiegelt somit in keiner Weise die Meinung der Europäischen Union.*



## Gliederung

- Einleitung und Motivation
  - COMO Teilprojekt B3: IT-Security Automotive
  - Beispiel Simulation zu Wurmepidemien: vom WLAN zum Automobil
  - Basisangriffe
- Methodik zur ganzheitlichen, pauschalisierten Betrachtung des Automobils und seines Umfelds
  - Pauschalisierung automotiver Systeme/Komponenten
  - Modellierung von Objekten und Beziehungen
  - Analyse von Sicherheitsanforderungen in Funktionsnetzentwürfen
  - Formalisierung der Sicherheitsanforderungen
  - Beispielhaftes Szenario eines automotiven integrierten Navigationssystems
- Zusammenfassung und Ausblick

siehe dazu auch die Veröffentlichung:
Sandro Schulze, Tobias Hoppe, Jana Dittmann, Gunter Saake: Pauschalisierte Sicherheitsbetrachtungen automotiver Systeme, erscheint in D.A.CH Security 2009, Ruhr-Universität Bochum, 19. und 20. Mai 2009



## Einleitung und Motivation

- IT-Sicherheit im Automobilbereich – warum?
  - Zunehmende Komplexität automotiver IT und Vernetzung. Klare Trends:
    - Ablösung mechanischer Komponenten durch elektronische Varianten (*X-by-Wire*)
    - drahtlose Kommunikation (Bluetooth, GSM, RFID, WLAN, C2C, C2I, …)
  - Langfristig ganzheitliche Konzepte automotive IT-Security erforderlich
  - Absichtliche Angriffe auf automotive IT und Besonderheiten verglichen mit Desktop-IT ...



## Einleitung und Motivation

- Absichtliche Angriffe auf automotive IT und Besonderheiten verglichen mit Desktop-IT:
  - Eingriffe können neben Beeinträchtigung des Komforts auch weiterreichende Einflüsse bis hin auf die Gesundheit und Leben der Verkehrsteilnehmer haben (Wechselwirkungen Safety vs. Security). Beispiele für Safety-kritische Komponenten: Energie- und Antriebssysteme, Airbag-Systeme etc.
  - Breites Spektrum von Angreifern und ihrer Motivationen: Tuner/Besitzer, Wettbewerber, Hacker, Spione, Saboteure, etc. (Betrachtung nach CERT)
  - Angriffsobjekt ist oft in voller physischer Kontrolle des Angreifers! (ähnlich Geldkarte) oder zukünftig direkt vernetzt: C2C, C2X, ...
  - Kaum Erfahrungswerte zu computerforensischen Aufklärungen bei automotiver IT



## Einleitung und Motivation

- Es ist zunehmend mit Angriffen auf die IT-Sicherheit zu rechnen!
- Beispiele:
  - Infektion eines Lexus-Onboard-Computers über ein Mobiltelefon
  - Angriff auf TMC-Daten: Einspielen gefälschter Verkehrsinfos über UKW
  - Km-Standsanzeigenmanipulation
    - Höherer Wiederverkaufswert
    - Serviceintervallverlängerung
  - „TV in motion hack" [TIM09] z.B. Vortäuschen des Handbremsensignals
    - Entfernen von TV-Restriktionen
    - Safety-Risiko durch unerwartete Lenkschloßauslösung/verriegelung
  - Manipulation von Hybridfahrzeugen [HYH06], z.B. Umgehen der Energiestatusprüfung


[Kas05] Eugene Kaspersky: *Viruses coming aboard?*, Viruslist.com Weblog-Eintrag vom 24.1.2005, http://www.viruslist.com/en/weblog?discuss=158190454&return=1

[BBO7] Andrea Barisani, Daniele Bianco: *Unusual Car Navigation Tricks: Injecting RDS-TMC Traffic Information Signals*, CanSecWest Vancouver 2007

[TIM09] Vertreiber von TV-in-Motion Manipulationskits, z.B. http://www.tv-in-motion.co.uk

[HYH09] *Hack Your Hybrid – Activate EV Stealth Mode, Get Rid of the BEEP, and More!*, http://www.treehugger.com/files/2006/01/hack_your_hybri.php



## Einleitung und Motivation
### Angriffe...

**2007:**

***Andreas Lang, Jana Dittmann, Stefan Kiltz, Tobias Hoppe: Future Perspectives:*** ***The Car and its IP-Address - A Potential Safety and Security Risk Assessment***; In: *Computer Safety, Reliability, and Security. Proceedings of the 26th International Conference SAFECOMP 2007*, S. 40-53, Springer LNCS 4680, ISBN 978-3-540-75100-7, Safecomp 2007, Nürnberg, September 2007

***Tobias Hoppe, Stefan Kiltz, Andreas Lang, Jana Dittmann: Exemplary Automotive Attack Scenarios:*** ***Trojan horses for Electronic Throttle Control System (ETC) and replay attacks on the power window system***; In: *Automotive Security - VDI-Berichte Nr. 2016, Proceedings of the 23. VDI/VW Gemeinschaftstagung Automotive Security*, S. 165-183, VDI-Verlag, ISBN 978-3-18-092016-0, 23. VDI/VW Gemeinschaftstagung, Wolfsburg, November 2007

**2008:**

***Tobias Hoppe, Jana Dittmann:*** ***Vortäuschen von Komponentenfunktionalität im Automobil: Safety- und Komfort-Implikationen durch Security-Verletzungen am Beispiel des Airbags***; In: *Sicherheit - Schutz und Zuverlässigkeit; Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)*, S. 341-353, ISBN 978-3-88579-222-2, Sicherheit 2008, Saarbrücken, April 2008

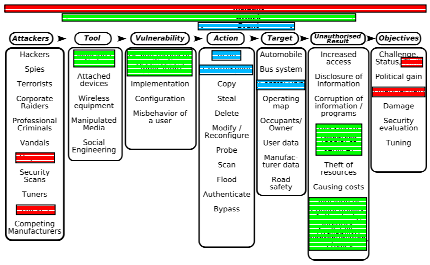
***Tobias Hoppe, Stefan Kiltz, Jana Dittmann:*** ***Security threats to automotive CAN networks – practical examples and selected short-term countermeasures***; In: *Computer Safety, Reliability, and Security, Proceedings of the 27th International Conference SAFECOMP 2008*, S. 235-248, Springer LNCS 5219, ISBN 978-3-540-87697-7, Safecomp 2008, Newcastle/UK, September 2008

***Tobias Hoppe, Stefan Kiltz, Jana Dittmann: Automotive IT-Security as a Challenge:*** ***Basic Attacks from the Black Box Perspective on the Example of Privacy Threats***; In: *escar - Embedded Security in Cars, 6th Conference*, escar 2008, Hamburg, November 2008

**2009:**

***Michael Biermann, Tobias Hoppe, Jana Dittmann, Sandro Schulze, Gunter Saake:*** ***Adaption des Szenarios einer WiFi-Wurm-Epidemie auf den Automotive-Bereich zur Sensibilisierung für und Aufklärung über das Bedrohungspotential***, erscheint in: *11. Deutscher IT-Sicherheitskongress des BSI*, BSI-Sicherheitskongress 2009, Bonn, Mai 2009

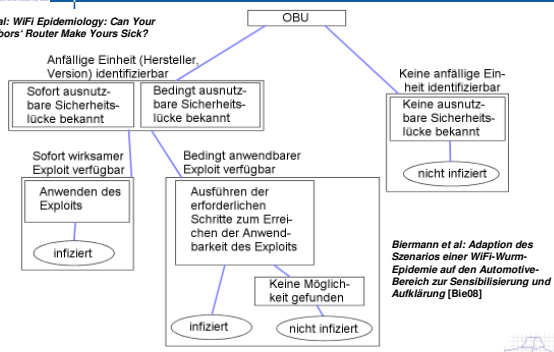
## Classification of attacks on automotive IT using an adapted CERT taxonomy






## Adaption von WiFi Wurm-Epidemien auf C2C

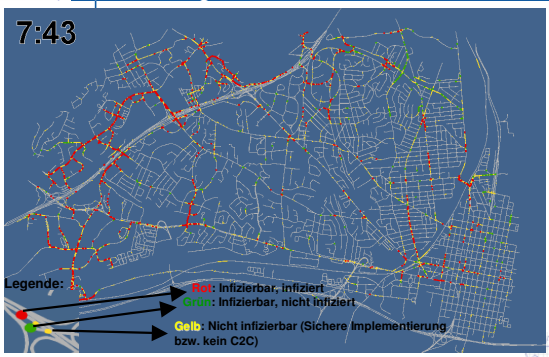
***Hu et al: WiFi Epidemiology: Can Your Neighbors' Router Make Yours Sick?*** **[Hu08]**




***Biermann et al: Adaption des Szenarios einer WiFi-Wurm-Epidemie auf den Automotive-Bereich zur Sensibilisierung und Aufklärung*** **[Bie08]**



## Einleitung und Motivation





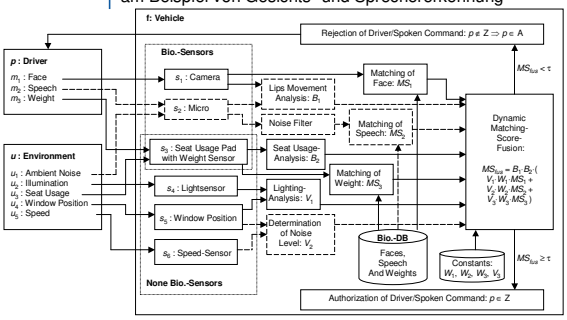

## COMO Teilprojekt B3: IT-Security Automotive
### Ziele und Schwerpunkte

- OvGU Forschungsschwerpunkt Automotive, Competence in Mobility (COMO)
- B3 betrachtet die Sicherheit von automotiven Systemen insbesondere unter dem Blickwinkel absichtlicher Angriffe (Prof. Dittmann, Prof. Saake, Prof. Jumar)
- Konkreten Arbeitspakete:
  - AP 1: Bedrohungsanalyse und Erarbeitung pauschalisierter Richtlinien und Designpattern


  - AP 2: Entwurf und Bearbeitung von Beispielszenarien
    - AP 2.1: Multimodale biometrische Authentifizierungssysteme am Beispiel von Gesichts- und Sprechererkennung
    - AP 2.2: Sicheres automotives Datenmanagement: Domänenanalyse am konkreten Beispiel des adaptiven Fahrwerks
    - AP 2.3: C2C-Kommunikation: Designpattern für sichere berührungslose Kommunikation
  - AP3: Evaluierung und Verifikation der entwickelten Pauschalisierungen, Restrisikoabschätzung



## Multimodale biometrische Authentifizierungssysteme am Beispiel von Gesichts- und Sprechererkennung

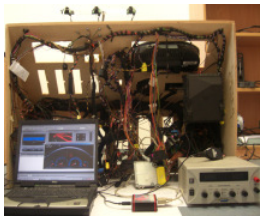




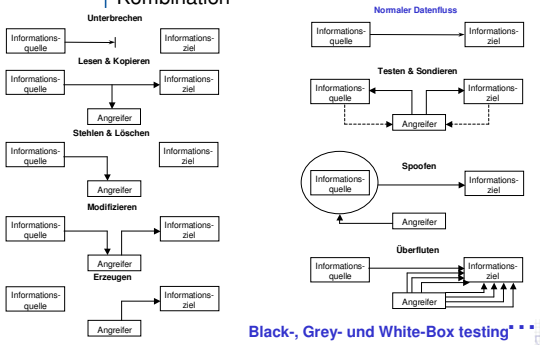

## COMO B3: Laborausstattung

Den praktischen Bezug der Arbeiten unterstützen Laboraufbauten automotiver IT-Komponenten aus verschiedenen Fahrzeugen großer internationaler Hersteller (z.B. Baujahre 2005, 2007) und automotive Entwicklungs- und Diagnoseprodukte

- Hersteller A, Baujahr 2004, CAN/LIN (siehe Bild), Hersteller A, Baujahr 2005, CAN/LIN
- Hersteller B, Baujahr 2007, CAN/MOST



## Grundlegende Angriffsstrategien und deren Kombination




**Black-, Grey- und White-Box testing**



## Funktionale Sicherheit, IT-Sicherheit und Komfort

- Funktionale Sicherheit

| | |
|---|---|
| SIL 1 | geringfügige Unfälle zu vermeiden |
| SIL 2 | ernsthaftere, aber im Ausmaß limitierte, Vorfälle zu vermeiden |
| SIL 3 | ernsthafte Unfälle zu vermeiden, die zahlreiche Todesopfer nach sich ziehen |
| SIL 4 | katastrophale Unfälle zu vermeiden. |

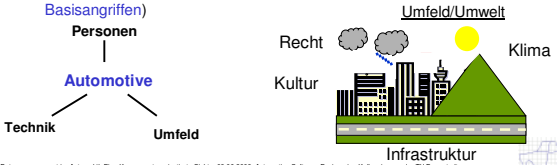
- IT-Sicherheit
  - Vertraulichkeit (*C*)
  - Integrität (*I*)
  - Verfügbarkeit (*A*)
  - Nicht-Abstreitbarkeit (*N*)
  - Authentizität (*U*)
- Komfortstufen

| | | |
|---|---|---|
| KS0 | Manuelle Bedienung des Systems | volle Ablenkung des Fahrers |
| KS1 | halbautomatische Bedienung des Systems | teilweise Ablenkung des Fahrers |
| KS2 | vollautomatische Bedienung des Systems | keine Ablenkung des Fahrers |



## Einleitung und Motivation

- Warum Pauschalisierung der Sicherheitsbetrachtungen?
  - Abstrakte Sicht auf funktionale und strukturelle Zusammenhänge
  - Nicht abhängig von konkreten Implementierungen
  - Konzept: mehrstufige Methodik – ein erster Ansatz
    - Pauschalisierung: durch Modellierung des Automotiven Systems (AS) bzw. dessen Einflussfaktoren
    - Formalisierung: durch beschreibende Gleichungen
  - Pauschalisierung auch von Angriffen möglich (Kombination von fünf Basisangriffen)



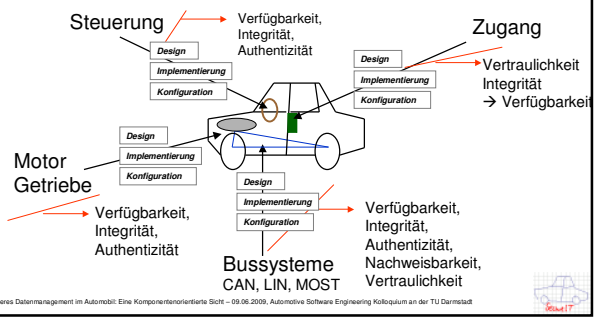






## Automotive pauschalisiert

Technisches Versagen– Rückführung auf Schwachstellen und Sicherheitsaspekte





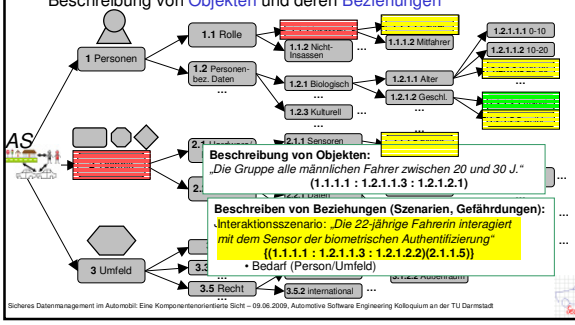

## Pauschalisierung automotiver Systeme

- Ansatz:
  - Definition abstrakter Sichten und Bausteine (analog zu BSI Grundschutz) speziell für das Anwendungsgebiet Automobil
- Pauschalisierte, formale Darstellung von
  - technischen Eigenschaften und Zusammenhängen automotiver Systeme - Technik
  - Wechselwirkungen / Interaktionen mit dem Menschen
  - übergreifender Randbedingungen des Umfelds
- Ziele:
  - Beschreibung von Objekten aus dem automotiven Umfeld
  - Beschreiben und Identifizieren von Beziehungen:
    - Szenarien, Gefahren (Safety + Security)
  - Abschätzung von Gefährdungswahrscheinlichkeiten und -potenzial
  - als Unterstützung bei der Definition von Schutzmaßnahmen



## Pauschalisierung und Modellierung von Objekten und Beziehungen

- Baumstruktur mit Bausteinen eines Automotiven Systems (AS) zur Beschreibung von Objekten und deren Beziehungen



## Beschreibung bedrohter Komponenten und ihrer gegenseitigen Abhängigkeiten

- Grundlage: *Logische* Sicht auf die Struktur automotiver Systeme
  - Abstrahieren von der detaillierten Struktur
  - Möglichkeit der Beschränkung auf Teilfunktionalitäten
- Modellierung von (Teil-)Funktionalitäten im AS durch Funktionsnetze (von Komponenten aus Abb. 1)
- Knoten: Komponenten des AS
  - Aus den Sichten Technik, Mensch, Umfeld
- Gerichtete Kanten: Datenfluss zwischen den Knoten (je Datum)
- Mögliche Rollen eines Knotens (pro Datum)
  - Provider: Bietet das Datum an bzw. leitet es weiter (Sender),
    - *PR* für dessen anforderbare Schutzziele (Sicherheitsaspekte)
  - Consumer: Nimmt ein Datum entgegen (Empfänger)
    - *CR* für dessen anforderbare Schutzziele (Sicherheitsaspekte)
  - Ein Knoten kann mehrere Rollen einnehmen



## Beispiele für Anwendungsdomänen

**Modellierung von Funktionsnetzen z.B. zu Funktionalitäten aus den Anwendungsdomänen:**

***Triebstrang/Fahrwerk***
- *Motorsteuerung*
- *Getriebesteuerung*
- *Fahrwerk*
- *ABS*
- *ESP*
- *Servolenkung*
- *Abstandsregelung*
- *…*

***Wartung/Diagnose***
- *Werkstatt-Tester*
- *Abgas-Tester*
- *Fertigungs-Tester*

***C2X***
- *C2C*
- *C2I*

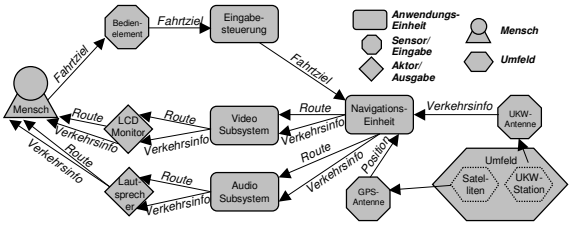
***Karosserie / Komfort***
- *Klimaanlage*
- *Scheibenwischanlage*
- *Bordnetz*
- *Sitzsteuerung und -heizung*
- *Lichtanlage*
- *Schließsystem*
- *Wegfahrsperre*
- *Schwingungs- und Schallreduktion*
- *…*

***Infotainment***
- *Instrumentenkombination*
- *Kassetten / CD-Radio*
- *CD/DVD Navigation*
- *Telefon / Freisprecheinrichtung*
- *TV-System*
- *Car-PC, Internet*



## Beispielhaftes Funktionsnetz

- Abstrahierte, logische Sicht auf ein integriertes Navigationssystem






## Propagation von Sicherheitsanforderungen in Funktionsnetzentwürfen

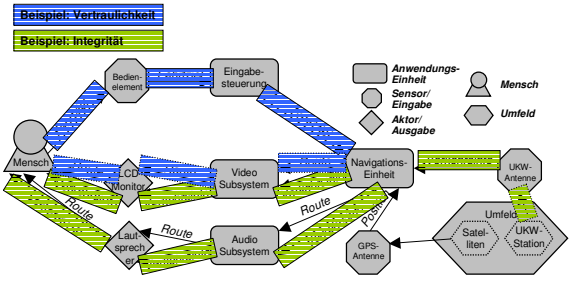
- Je nach Datum können gewisse Schutzziele gefordert sein
- Die Funktionsnetzmodellierung hilft bei
  - ⇨ der Identifikation der betroffenen Komponenten
  - ⇨ Dem Ableiten weiterer Anforderungen, die die Sicherstellung der Schutzeigenschaften unterstützen
- Beispiel 1: Anforderung „Vertraulichkeit“:
  - In der Regel von der Quelle des Datums gestellt, die Empfänger
    - müssen über geeignete *Maßnahmen* für die Vertraulichkeit des Datums sorgen.
    - übernehmen die Schutzanforderung und dürfen das Datum (oder abgeleitete Werte, die zurückschließen lassen) nur in geschützter Form weiterübermitteln.
- Beispiel 2: Anforderung „Integrität“:
  - In der Regel vom Empfänger eines Datums gestellt, die Sender
    - müssen geeignete Maßnahmen zur Überprüfbarkeit der Integrität bereitstellen.
    - müssen die Anforderung für alle relevanten Eingabedaten übernehmen, die so an deren Quellen weitervererbt wird.



## Propagation von Sicherheitsanforderungen in Funktionsnetzentwürfen - Beispiele

**Beispiel: Vertraulichkeit**

**Beispiel: Integrität**






## Relevanz von Sicherheitsmodellen

- Beispiel zeigt: Aussagen zu Aspekten des Zugriffsschutzes anhand des Informationsflusses möglich
- Beachte: Relevanz von formalen Sicherheitsmodellen, z.B.
  - Multi-Level Sicherheitsmodelle
    - ⇨ *Bell-LaPadula* (Vertraulichkeit), *Biba* (Integrität)
    - Potentielle Eignung im automotiven Kontext, z.B:
      - Zuweisung von Schutzstufen an Daten und Komponenten
  - Multilaterale und weitere Sicherheitsmodelle
    - ⇨ *Chinese-Wall*, *Clark-Wilson*
    - Berücksichtigung, dass viele Komponenten unterschiedlichen Informationsflüssen beteiligt sind

⇨ Gegenstand weiterer Forschung

## Formalisierung: Ziel und Ansatz

- Ziel: Aussagen über Schutzziele von Daten (Ressourcen) auf den einzelnen Komponenten mit formalen Mitteln
- Idee: Funktionsnetze (log. Sicht) um Schutzziele ergänzen
- Abhängigkeiten im Funktionsnetz für Delegation der Schutzziele ausnutzen
- Abstraktion des Funktionsnetzes zu einem *gerichteten Graphen* → Graphentheorie anwendbar
- Schutzziele in unterschiedlicher Granularität bestimmbar einschließlich erforderliches Schutzniveau



## Formalisierung: Basisdefinitionen

- Menge aller Knoten (*vertices*) im AS-Baum $V = \{v_1,\ldots v_{nv}\}$
  - z.B. ECU, Sensor, Aktor):
- Menge aller (ausgetauschten) Daten (*data*) $D = \{d_1,\ldots d_{nd}\}$
- Menge aller Kanten (*edges*): $E = \{e_1,\ldots e_{ne}\}$ mit
  - dem Tripel $e_i=\{v_j, v_k, d_i\}$ als eine bestimmte Kante (*edge*)
  - $\{v_j,v_k\} \in E$ = verbundene Knoten
  - $d$ das kommunizierte Datum
- Menge aller Graphen (*graph*) : $G = \{G_1,\ldots G_{ng}\}$ mit
  - $G_m = \{V_m \subset V, E_m \subset E, s_m, t_m, d_m \in D\}$ als ein Graph zu einem Datum $d_m$
  - den Funktionen $s_m$, $t_m$: $E \mapsto V$, die den Kanten ihren Quell (*source*) bzw. Zielknoten (*target*) zuordnen
- Menge aller Funktionsnetze $F = \{f_1,\ldots,f_{nf}\}$ mit $f_i = \{G_i \subset G\}$ als einzelnes Funktionsnetz (*function net*)
- Menge der Schutzziele (*security aspects*): $S = \{C, I, A, U, N, P\}$



## Formalisierung: Basisdefinitionen (cont.)

- Schutzziele durch Datenfluss im FN tlw. gegeben

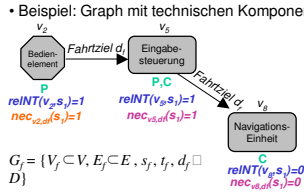
| Schutzziele (Sicherheitsaspekte) | Anforderung meist von | Maßnahmen meist durch |
|---|---|---|
| Vertraulichkeit (*C*; Confidentiality) | Provider | Beide |
| Integrität (*I*; Integrity) | Consumer | Beide |
| Verfügbarkeit (*A*; Availability) | Consumer | Provider |
| Authentizität (*U*; Authenticity) | Consumer | Beide |
| Nichtabstreitbarkeit (*N*; Non-repudiation) | Beide | Beide |
| Datenschutz (*P*; Privacy) | Provider | Provider, ggf. Consumer |

- Anforderbare Schutzziele für die Knotentypen, z.B.:
  - Consumer → $CR \subset S = S / \{C, P\}$
  - Provider → $PR \subset S = S / \{I, A, U\}$



## Formalisierung: Bestimmung der Schutzziele - Eine datenorientierte Sichtweise

- Voraussetzung: Funktionsnetze für das gesamte AS sind erstellt
- Jedes Funktionsnetz pro Datum in Graphen zerlegen
- Ziel: Formale Bestimmung der Schutzziele für alle Knoten
- Beispiel: Graph mit technischen Komponenten zum Datum „Fahrtziel" ($d_f$):




$G_f = \{V_f \subset V, E_f \subset E, s_f, t_f, d_f \in D\}$

Aus dem Graph ergeben sich:
- ***Knotentypen*** (*P*=Provider, *C*=Consumer) für das betrachtete Datum
- Unmittelbare ***Relevanz*** des Schutzziels $relNT(v_i,s_j)$ ⇨ $s_j \in CR$ bzw. $s_j \in PR$ ?

Weitere Schritte:
- Festlegen **notwendiger Schutzziele** für initiale Knoten mittels $nec_{v,df}(s_j)$
- Iterative **Weitervererbung** der Schutzziele des Datums auf weitere Knoten über *delegate*($v_n$,$v_m$,$s_j$)

- Anschließend: Graphen wieder zum Funktionsnetz zusammenführen
- Welche Knoten sollten welche Maßnahmen implementieren? ⇨ Funktion *fulfill*

⇨Teil weiterer Forschung. Im Beitrag: erster Brute-Force-Ansatz



## Zusammenfassung/Ausblick

- Zusammenfassung:
  - Pauschalisierung von Bausteinen automotiver Systeme zur Modellierung von Objekten und Beziehungen
  - Aufbauende Spezifikation von datenorientierten Funktionsnetzen und Untersuchungen zu Sicherheitsanforderungen und –modellen
  - Formalisierung und Anwendung zur Ermittlung von Schutzzielen
- Ausblick:
  - Generell:
    - Nähere Einbeziehung von Sicherheitsmodellen
    - Demonstration an weiteren Anwendungsbeispielen, z.B. Nutzen für Datenschutz bei der Integration automotiver biometrischer Anwendungen
  - Formalisierung:
    - Abdecken von abgeleiteten Daten
    - Schutzziele ganzheitlich, semi-automatisch zu erfassen
    - Erweiterte Graphenmodelle (z.B. attributierte Graphen)
    - Berücksichtigung von Schutzmaßnahmen



**2007:**

**[1] *Andreas Lang, Jana Dittmann, Stefan Kiltz, Tobias Hoppe: Future Perspectives: The Car and its IP-Address - A Potential Safety and Security Risk Assessment***; In: *Computer Safety, Reliability, and Security. Proceedings of the 26th International Conference SAFECOMP 2007*, S. 40-53, Springer LNCS 4680, ISBN 978-3-540-75100-7, Safecomp 2007, Nürnberg, September 2007

**[2] *Tobias Hoppe, Jana Dittmann: Sniffing/Replay Attacks on CAN Buses: A Simulated Attack on the Electric Window Lift Classified using an Adapted CERT Taxonomy***; In: *CD-Proceedings of the 2nd Workshop on Embedded Systems Security (WESS'2007), A Workshop of the IEEE/ACM EMSOFT'2007 and the Embedded Systems Week*, WESS 2007, Salzburg, Oktober 2007

**[3] *Tobias Hoppe, Stefan Kiltz, Andreas Lang, Jana Dittmann: Exemplary Automotive Attack Scenarios: Trojan horses for Electronic Throttle Control System (ETC) and replay attacks on the power window system***; In: *Automotive Security - VDI-Berichte Nr. 2016, Proceedings of the 23. VDI/VW Gemeinschaftstagung Automotive Security*, S. 165-183, VDI-Verlag, ISBN 978-3-18-092016-0, 23. VDI/VW Gemeinschaftstagung, Wolfsburg, November 2007

**2008:**

**[4] *Sandro Schulze, Stefan Kiltz, Tobias Hoppe, Jana Dittmann: Modelling Data Requirements for a Secure Data Management in Automotive Systems***; In: *Tagungsband des Workshops "Modellbasierte Entwicklung von eingebetteten Fahrzeugfunktionen"*, Modellierung 2008, Berlin, März 2008

**[5] *Andrey Makrushin, Jana Dittmann, Stefan Kiltz, Tobias Hoppe: Exemplarische Mensch-Maschine-Interaktionsszenarien und deren Komfort-, Safety- und Security-Implikationen am Beispiel von Gesicht und Sprache***; In: *Sicherheit - Schutz und Zuverlässigkeit; Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)*, S. 315-327, ISBN 978-3-88579-222-2, Sicherheit 2008, Saarbrücken, April 2008

**[6] *Tobias Hoppe, Jana Dittmann: Vortäuschen von Komponentenfunktionalität im Automobil: Safety- und Komfort-Implikationen durch Security-Verletzungen am Beispiel des Airbags***; In: *Sicherheit - Schutz und Zuverlässigkeit; Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)*, S. 341-353, ISBN 978-3-88579-222-2, Sicherheit 2008, Saarbrücken, April 2008

**[7] *Tobias Hoppe, Stefan Kiltz, Jana Dittmann: IDS als zukünftige Ergänzung automotiver IT-Sicherheit***; In: *DACH Security 2008; Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven*, S. 196-207, Syssec, ISBN: 978-3-00-024432-6, DACH Security 2008, Berlin, Juni 2008,

**[8] *Tobias Hoppe, Stefan Kiltz, Jana Dittmann: Adaptive Dynamic Reaction to Automotive IT Security Incidents using Multimedia Car Environment***; In: *The Fourth International Symposium on Information Assurance and Security (ias 2008)*, S. 295-298, IEEE computer society, ISBN: 0-7695-3324-7, ias 2008, Neapel/Italien , September 2008

**[9] *Michael Biermann, Tobias Hoppe, Jana Dittmann, Claus Vielhauer: Vehicle Systems: Comfort & Security Enhancement of Face/Speech Fusion with Compensational Biometrics***; In: *MM&Sec'08 - Proceedings of the Multimedia and Security Workshop 2008*,S.185-194, ACM, ISBN 978-1-60558-058-6, MM&Sec'08, Oxford/UK, September 2008

**[10] *Tobias Hoppe, Stefan Kiltz, Jana Dittmann: Security threats to automotive CAN networks – practical examples and selected short-term countermeasures***; In: *Computer Safety, Reliability, and Security, Proceedings of the 27th International Conference SAFECOMP 2008*, S. 235-248, Springer LNCS 5219, ISBN 978-3-540-87697-7, Safecomp 2008, Newcastle/UK, September 2008

**[11] *Tobias Hoppe, Stefan Kiltz, Jana Dittmann: Automotive IT-Security as a Challenge: Basic Attacks from the Black Box Perspective on the Example of Privacy Threats***; In: *escar - Embedded Security in Cars, 6th Conference*, escar 2008, Hamburg, November 2008


AMSL
Annual Multimedia and Security Lab
2009:
[12] Sandro Schulze, Mario Pukall, Gunter Saake, Tobias Hoppe, Jana Dittmann: On the Need of Automotive Data Management; In: Proceedings 13. GI-Fachtagung Datenbanksysteme für Business, Technologie und Web (BTW), Lecture Notes in Informatics. Gesellschaft für Informatik (GI), Münster, März 2009
[13] Michael Biermann, Tobias Hoppe, Jana Dittmann, Sandro Schulze, Gunter Saake: Adaption des Szenarios einer WiFi-Wurm-Epidemie auf den Automotive-Bereich zur Sensibilisierung und Aufklärung; In: Sichere Wege in der vernetzten Welt: Tagungsband zum 11. Deutschen IT-Sicherheitskongress; Secufledia Verlag Ingelheim, ISBN 978-3-922746-97-3, Mai 2009
[16] Sandro Schulze, Tobias Hoppe, Jana Dittmann, Gunter Saake: Pauschalisierte Sicherheitsbetrachtungen automotiver Systeme; In: Patrick Horster (Ed.), DACH Security 2009; Bochum; 19.-20. Mai 2009;
[15] Sandro Schulze, Mario Pukall, Tobias Hoppe: IT Security in Automotive Software Development; Erscheint in: Workshop der Gesellschaft für Informatik(GI) Entwicklung zuverlässiger Software-Systeme, 18. Juni 2009, Regensburg
[14] Tobias Hoppe, Stefan Kiltz, Jana Dittmann: Automotive IT-Security as a Challenge: Basic Attacks from the Black Box Perspective on the Example of Privacy Threats; To appear in: The 28th International Conference on Computer Safety, Reliability and Security - SAFECOMP 2009, Hamburg, Germany, 15-18 September 2009;
Sicheres Datenmanagement im Automobil: Eine Komponentenorientierte Sicht – 09.06.2009, Automotive Software Engineering Kolloquium an der TU Darmstadt