

# Ableitung von a priori Policies zum Schutz von Bordnetzen in Fahrzeug vor Angriffen aus dem Internet

Vortrag von secunet Automotive Security auf dem 12. Deutschen IT-Sicherheitskongress vom 10.-12. Mai 2011 in Bonn

## Kurzfassung:

Moderne Fahrzeuge sind durch die zunehmende Anzahl von Anwendungsfällen, die einen Online Zugang erfordern, vor ernsthafte Herausforderungen gestellt. Denn damit werden Bordnetze unbekanntem Angriffen aus dem Internet ausgesetzt. Es wird eine Methode vorgestellt, um mit Hilfe einer verhaltensbasierten Policy auf Standard Automotive Hardware unautorisierte Interaktion zwischen unbekannter Malware und dem Fahrzeugbordnetz zu unterbinden.

## Stichworte:

Embedded Security, Bordnetze, Policies, Internet-Zugang, Online-Zugang, Fahrzeug, Automobil

## 1. Einführung

Moderne Fahrzeuge sind nicht mehr ohne eine beträchtliche Anzahl von elektronischen Komponenten denkbar. So kann die Anzahl der Kleinrechner, sogenannte ECUs (Electronic Control Unit), in aktuellen Fahrzeugen bis zu 80 Einheiten betragen. Über die Programmierbarkeit dieser embedded Systeme sind schnelle Innovationszyklen realisierbar, indem aufwendige und langsame Entwicklungszyklen für Hardware durch eine Softwareentwicklung ersetzt werden, die komplexe Funktionen in Fahrzeugen vergleichsweise schnell realisieren kann, mit der Möglichkeit, diese Funktion im Nachhinein zu ändern, sei es in der Werkstatt oder in Zukunft auch über Fernwartungszugänge.

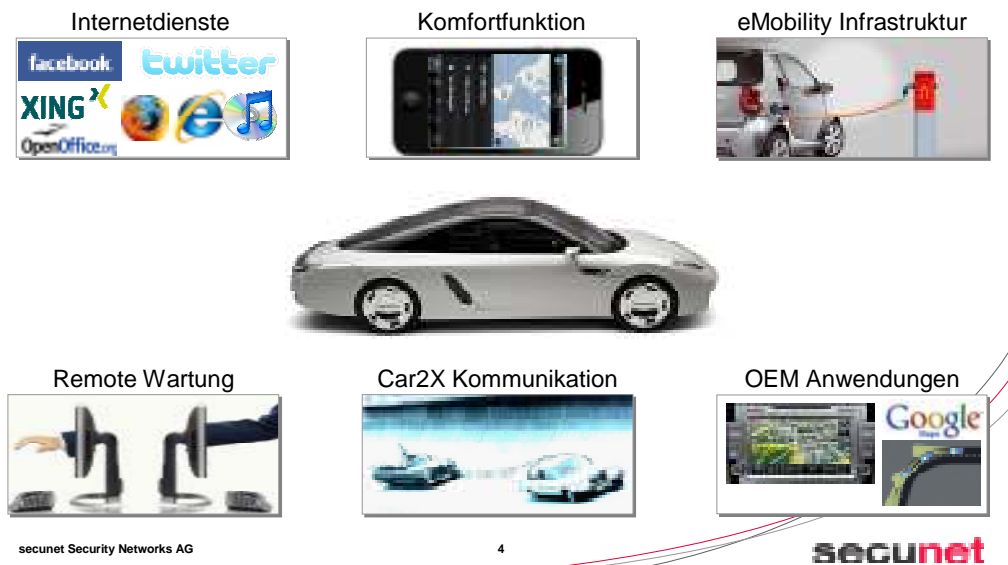
Neben dem Einsatz von Software im Fahrzeug trägt ein weiteres Merkmal moderner Autos zur stetigen Funktionsmehrung und Erhöhung der Safety bei. Durch die Vernetzung der einzelnen ECUs über Fahrzeugbusse können Funktionen auf alle Informationen zugreifen, die Fahrzeuge aus ihrer Umwelt über Sensoren aufnehmen. Damit sind kosteneffizient Funktionen wie ABS oder ESP realisierbar, aber auch fortgeschrittene Fahrerassistenzsysteme wie etwa das selbständige Bremsen im unteren Geschwindigkeitsbereich, wenn Personen auf die Fahrbahn laufen, oder etwa Spurhalteassistenten.

Im Streben nach neuen differenzierenden Funktionen, sei es im Komfort- aber auch im Safety Bereich macht die Vernetzung des Fahrzeugs vor externen Quellen nicht Halt. So werden zukünftige Fahrzeuge safety-relevante

Fahrdaten mit Hilfe der sogenannten Car-to-Car oder Car-to-Infrastructure Kommunikation mit anderen Fahrzeugen austauschen, um ein noch weiterreichendes Bild vom aktuellen Zustand seiner Umwelt zu erhalten, um noch sensibler auf mögliche kritische Fahrsituationen vorbereitet zu sein.

Wie bereits oben erwähnt halten auch Fernwartungszugänge immer mehr Einzug in die Fahrzeugwelt, um Daten aus dem Fahrzeug auszulesen und dem Fahrer oder einer Werkstatt auch ohne physikalischen Zugang zum Fahrzeug Informationen über den Zustand des Fahrzeugs zu liefern. Für die Zukunft werden in der Automobilindustrie aber bereits heute die Konzepte diskutiert, wie auch eine Fernprogrammierung des Fahrzeugs sicher möglich ist, um beispielsweise Wartungsarbeiten an der Software vornehmen zu können. Ein Vorgang der heutzutage jedem durch das Einspielen von Updates auf seinen Computer geläufig ist. Die nachfolgende Abbildung zeigt beispielhaft eine Übersicht der möglichen UseCases im Automobilumfeld, die in Zukunft eine Online Verbindung des Fahrzeugs notwendig machen. Insbesondere Internetdienste im Fahrzeug treiben diese Entwicklung.

### Online-basierte Dienste im Fahrzeug – Beispiele



**Abbildung 1: Beispiele für Online-Basierte Dienste im Fahrzeug**

Denn in konsequenter Fortführung des Gedankens, durch Software in immer kürzeren Zyklen dem Fahrer neue und ansprechende Funktionen insbesondere im Komfortbereich zu bieten, hält nun auch das Internet und die Anbindung des Fahrzeugs an App Stores Einzug in die Automobilwelt. Durch den Einsatz von Browsern, Widgets, der Anbindung von Consumer Electronics Geräten wie dem iPhone und durch das Einspielen von Apps in Infotainment

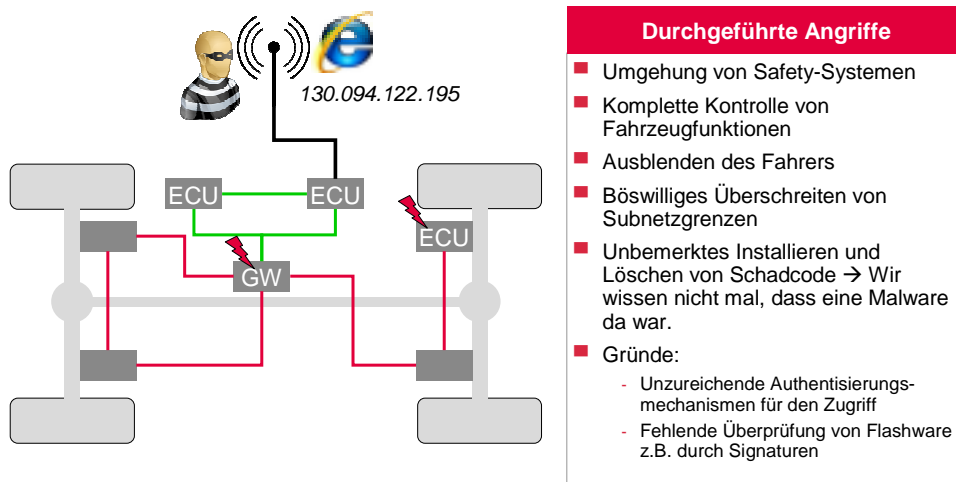
ECUs selbst, stehen einem Fahrzeughersteller schier unbegrenzte Ressourcen für die Entwicklung von Funktionen zu Verfügung. VW und die deutsche Telekom haben dies durch ihre Wettbewerbe „App my ride“ bzw. Telekom App Award praktisch gezeigt.

Demgegenüber stehen aber insbesondere Herausforderungen zur Aufrechterhaltung der Security wie sie aus dem Smartphone Umfeld schon seit längerem bekannt sind.

## 2. Sicherheitsziele für vernetzte Fahrzeuge

In Zukunft werden nicht mehr alle Applikationen, die über das Internet in ein Fahrzeug geladen werden können, auf eine Art und Weise getestet werden können, wie es heute für Fahrzeug-Software der Fall ist. Damit können solche komplexen Applikationen Hintertüren oder Exploits enthalten, die dann wiederum Sicherheitslücken der Betriebssysteme der Infotainment ECUs ausnutzen können, um auf die Bordnetze und damit Safety relevante Bereiche des Fahrzeugs Einfluss zu nehmen. Die Software eines Infotainmentsystems könnte also wie am PC über Software aus dem Internet angegriffen werden und aufgrund der oben erwähnten Vernetzung der ECUs in einem Bordnetz, können diese Angriffe auch fahrkritische Systeme erreichen. Welche Angriffe möglich sind, zeigt die nachfolgende Graphik (mehr dazu siehe [1])

### Hackerangriffe auf Fahrzeuge – Beispiel aus der Praxis



<http://www.autosec.org/pubs/cars-oakland2010.pdf>

secunet Security Networks AG

11

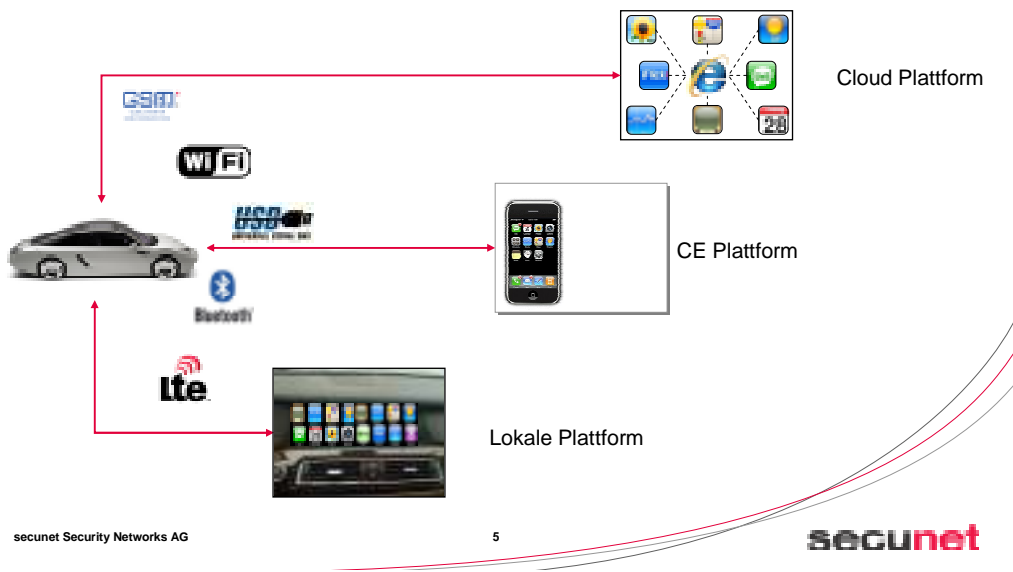
secunet

Abbildung 2 Beispiele für Hackerangriffe auf Fahrzeuge

Als zusätzliche Herausforderung, die es für die Fahrzeugindustrie zu meistern gilt, steht die Skalierbarkeit der Angriffe im Raum, d.h. ein erfolgreicher Angriff auf ein einzelnes Fahrzeug kann auf eine gesamte Fahrzeugflotte ausgedehnt werden.

Dabei zeigt die nachfolgende Abbildung, über welche Kanäle Angriffe an die Fahrzeuge gelangen können:

### Plattformen für Online-Dienste im Fahrzeug



**Abbildung 3: Übersicht der Zugänge und Online – Plattformen in Fahrzeugen**

Zugänge werden dabei über Standardschnittstellen wie USB oder WiFi hergestellt, die damit einer breiten Hackergemeinde bekannt sind. Die Möglichkeiten, Schadcode auf das Fahrzeug wirken zu lassen reichen vom Einsatz von Browsern (Cloud Plattform) als Möglichkeit Internet-Dienste ins Fahrzeug zu bringen, über die Anbindung von mobilen Endgeräten wie Smartphones oder Tablet PCs bis hin zu embedded Lösungen im Fahrzeug, die eine Möglichkeit bieten, Applikationen ins Fahrzeug herunterzuladen und dort zur Ausführung zu bringen.

Um auf solche Szenarien optimal vorbereitet zu sein, müssen die folgenden Sicherheitsziele erfüllt sein:

- Schutz der Integrität des Bordnetzes, um die Safety des Fahrzeugs zu jedem Zeitpunkt zu gewährleisten,

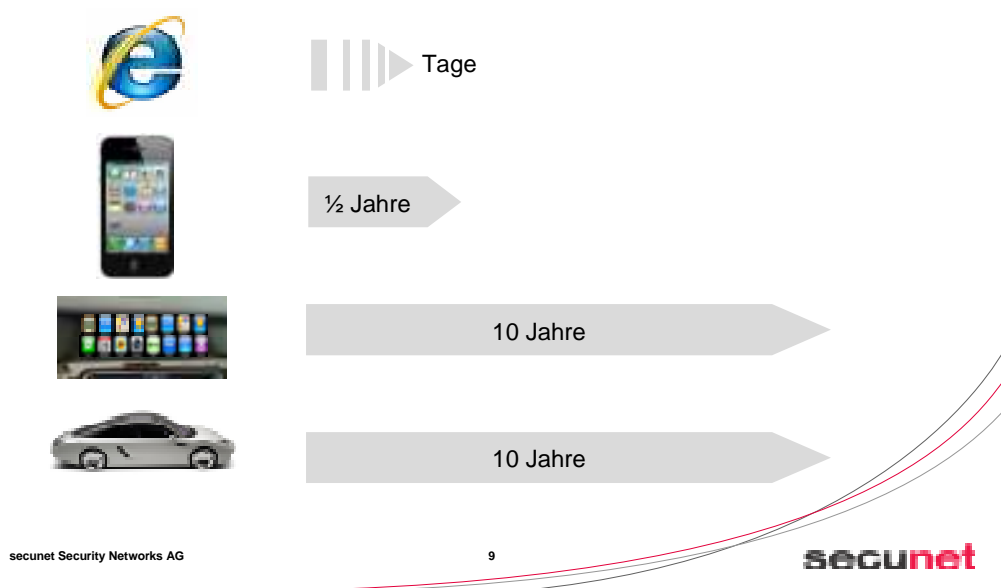
- Schutz der Vertraulichkeit persönlicher Daten, um Angreifer nicht in die Lage zu versetzen, durch fahrzeugbezogene Daten auf Personen schließen zu können, und
- Schutz der Verfügbarkeit der Plattform, um das Image und die Akzeptanz einer Infotainment Plattform nicht zu gefährden.

### 3. Lösungsansatz durch a priori Policies

Die großen Herausforderungen sind dabei die unbekanntenen Angriffe und Exploits, die über den Lebenszyklus eines Fahrzeugs mit höchster Wahrscheinlichkeit auftreten werden. Dies ist bereits durch die Komplexität der zugrundeliegenden Betriebssysteme gegeben. Allerdings sind die bekannten Ansätze aus der klassischen IT aufgrund der möglichen Schadenshöhe (Gefahr für Leib und Leben der Fahrzeuginsassen) nicht anwendbar, da hier das Risiko etwaiger Zero-Day-Exploits nicht vernachlässigt werden kann.

Die Gefahr von Zero-Day Exploits in Fahrzeuge wird anhand der nachfolgenden Abbildung deutlich:

#### Komplexität & Dynamik – Unterschiedliche Lebenszyklen



**Abbildung 4: Unterschiedliche Entwicklungszyklen in der Automobilindustrie**

Fahrzeuge und die entsprechenden embedded Systeme in denselben haben einen Lebenszyklus von ca. 10 Jahren. Im Gegensatz dazu ändern sich die über Browser verfügbaren Inhalte täglich bis stündlich und bei den Mobilien Endgeräten sind halbjährliche Entwicklungszyklen normal. Für die Fahrzeuge

bedeutet dies, dass nach einer ca. drei jährigen Entwicklungszeit für alle Funktionen des Bordnetzes, auch der Security, Angreifer 7 Jahre Zeit haben, Lücken zu finden. Am Beispiel eines Linux-basierten Infotainment Systems eines Fahrzeug bedeutet dies, dass alle Exploits, die nach der Beendigung der Designphase des Infotainment Systems auftreten, in einem Sicherheitskonzept, das in der Designphase des Fahrzeugs erstellt wurde, nicht enthalten sind. Denn eine solches Sicherheitskonzept kann natürlich die bekannten Angriffe berücksichtigen und Annahmen über die Zukunft treffen. Es aber bleibt ein nicht unerhebliches Restrisiko, dass entscheidende Exploits nicht berücksichtigt wurden. Dabei spielt es keine Rolle, ob es sich um Linux oder eine anderes Infotainment Betriebssystem handelt, da jedes hinreichend komplexe Betriebssystem aufgrund der immensen Anzahl von Lines of Code notwendigerweise Schwachstellen enthält. Sicherheitsbewertung veralten demnach relativ schnell und berücksichtigen neue Bedrohungen nicht zufriedenstellend. Vor dem Hintergrund der oben bereits angesprochenen resultierenden Gefahr für Leib und Leben der Passagiere besteht hier Handlungsbedarf für eine weitergehende Absicherung von Bordnetzen. Was also benötigt wird, ist ein Ansatz, der eine vollständige Risikoklassifizierung aller Applikationen, auch der unbekanntes, ermöglicht. Dieser Ansatz wird wie nachfolgend dargestellt als Trust Level Ansatz bezeichnet.

### Ansatz über Trust Levels im Automobilumfeld

- Exploits sind immer erst im Nachhinein bekannt
- Eine Sicherheitsbewertung ist schwierig und noch schneller veraltet
- Neue Bedrohungen können nicht berücksichtigt werden (siehe Komplexität&Dyn.)



#### Trust Level

- Vollständige Risikoklassifizierung von Applikationen und Daten VOR dem Einsatz im Fahrzeug
- Klares Spektrum: kein Vertrauen vs. volles Vertrauen
- Die Klassifikation erfolgt über den Umfang der mit dem Bordnetz austauschbaren Informationen

**Abbildung 5: Trust Level Ansatz zur Klassifizierung von Applikationen und Daten**

Mit diesem Ansatz kann sowohl bekannten als auch unbekanntes Applikationen, Aktoren (Z.B. Server, Zugangsinterfaces, Personen ...) und

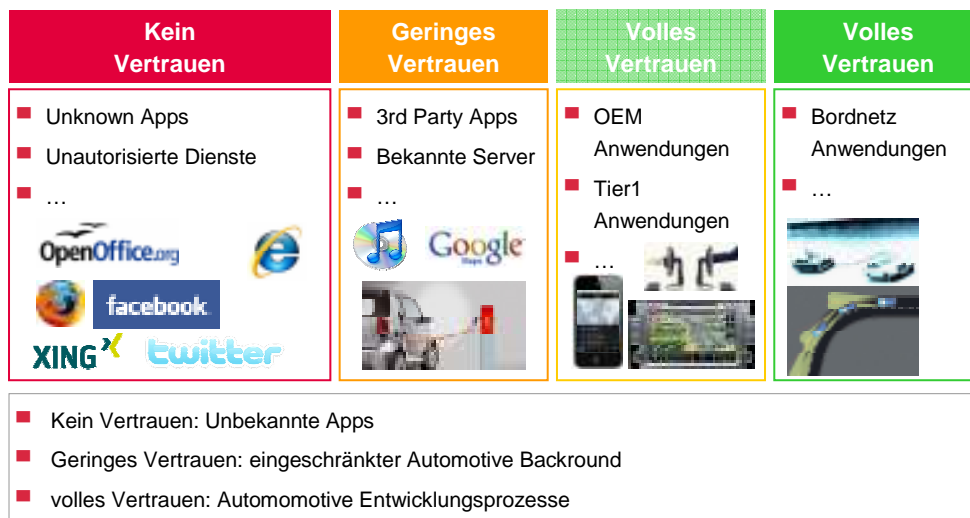
Daten ein Trust Level zugeordnet werden. Denn unbekanntem Applikationen, Aktoren und Daten kann immer das Trust Level „kein Vertrauen“ zugeordnet werden. Im folgenden verwenden wir eine dreistufige Klassifizierung, die vor allem die Quellen von Applikationen berücksichtigt.

Das Trust Level „kein Vertrauen“ wurde bereits oben charakterisiert.

Geringes Vertrauen wird Applikationen und Diensten entgegengebracht, die einem Fahrzeug zwar authentisiert werden können, aber nicht vom Fahrzeughersteller oder einem Tier1 – Zulieferer erstellt wurden. Typischerweise handelt es sich hier um Server mit gültigem Zertifikat und 3rd – Party – Applikationsentwickler.

„Volles Vertrauen“ hingegen genießen Applikationen und Dienste, die von den Fahrzeugherstellern bzw. den Tier1-Zulieferern selbst entwickelt und betrieben werden. Hier kann auch vorausgesetzt werden, dass entsprechende automotiv Entwicklungsprozesse vorhanden sind, um insbesondere das in Kapitel 2 genannte Sicherheitsziel der Integrität des Bordnetzes nicht zu verletzen. Beispiele für die Klassifikation von Applikationen finden sich in der nächsten Abbildung:

### Klassifikation der Applikationen hinsichtlich Vertrauen



secunet Security Networks AG

8

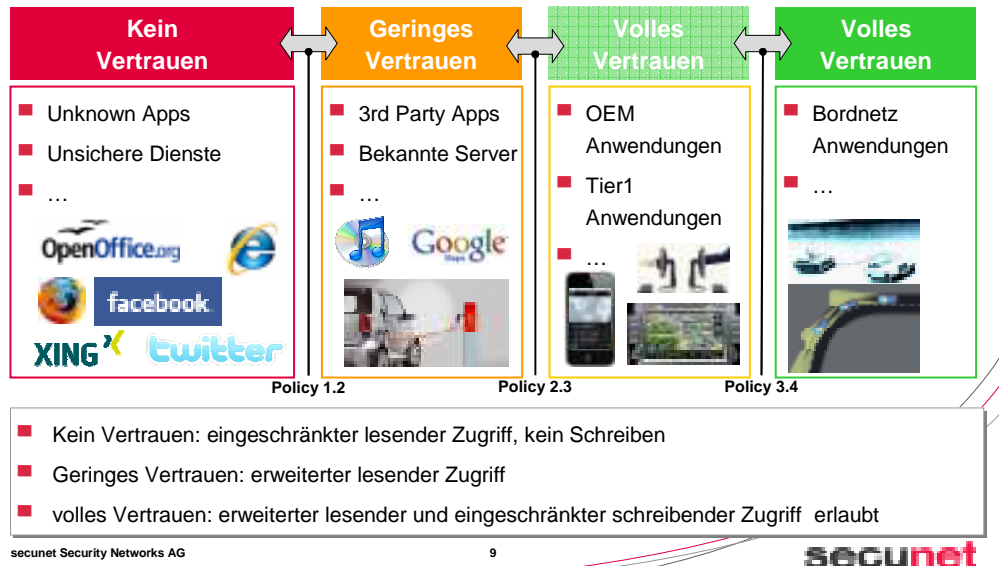
secunet

**Abbildung 6: Schema zur Trust Level Klassifikation von Applikationen und Diensten**

Ein Menge von Applikationen und Diensten, die das gleiche Trust Level haben, werden zu einer sogenannten Trustdomain zusammengefasst. Diese Trustdomains zeichnen sich dadurch aus, dass sich diese Domänen gegenseitig nicht beeinflussen können und die Interaktion zwischen den

Domänen auf den Austausch von Nachrichten beschränkt ist. Welche Nachrichten dabei erlaubt sind, wird durch Regelwerke, sogenannte Policies, festgelegt, wie in der nachfolgenden Abbildung dargestellt ist:

### Ableitung einer a priori Policy pro Trust Domain

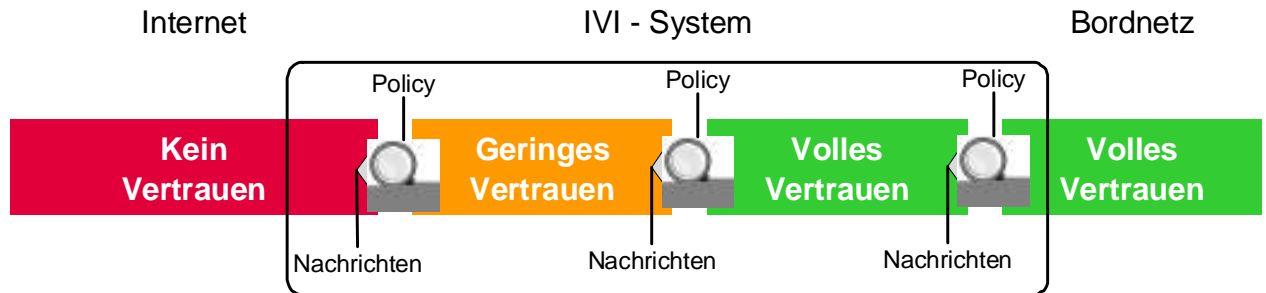


**Abbildung 7: A priori Policies für eine sichere Kommunikation mit dem Bordnetz**

Auf das Fahrzeug bezogen bedeutet dies, dass aufbauend auf der Spezifikation des Bordnetzes festgelegt wird, welche Nachrichten, aus welcher Trustdomain an das Fahrzeug-Bordnetz gesendet werden darf. Da die Festlegung dieser Policies vor der Installation von potentiellen Applikationen und Diensten im Fahrzeug erfolgt und unabhängig von diesen Applikationen und Diensten ist, werden diese Policies a priori Policies genannt. Ein Beispiel für eine a priori Policy für den Zugriff einer Trustdomain auf das Fahrzeugbordnetz könnte wie folgt aussehen:

- Trustdomain „Kein Vertrauen“: eingeschränkter lesender Zugriff, kein Schreiben auf das Bordnetz
- Trustdomain „Geringes Vertrauen“: erweiterter lesender Zugriff auf das Bordnetz
- Trustdomain „volles Vertrauen“: erweiterter lesender und eingeschränkter schreibender Bordnetz-Zugriff erlaubt

Daraus lässt nun wie in der nächsten Abbildung dargestellt ein Ansatz für sichere In-Vehicle-Infotainment (IVI) Systeme ableiten. Eine detailliertere a priori Policy ist konkreten Fahrzeug-Bordnetz erstellt werden.



**Abbildung 8: Abgeleitete sichere IVI Systeme in Fahrzeugen durch Trustdomains**

Ein solches IVI System stellt pro Trustdomain eine Ablaufumgebung zur Verfügung, in der jeweils Applikationen und Dienste des zugehörigen Trustlevels installiert werden. Das IVI System muss dafür sorgen, dass die Partitionen sich nicht gegenseitig beeinflussen und diese Abgrenzung auch durch Angriffe innerhalb der Partition nicht verloren geht. Zudem sollen Applikationen können die zugewiesene Trustdomain nicht verlassen können, d.h. zwischen benachbarten Trustdomains werden nur Nachrichten, kein Code ausgetauscht. Da in Verbindung mit der oben genannten Abgrenzung Angriffe auf das Bordnetz nur durch Kommunikation (Nachrichten) erfolgen können, werden diese von der Policy vollständig kontrolliert. Die Kontrolle erfolgt unabhängig von den Anwendungen und beruht nur auf Informationen über die Funktionsweise des Bordnetzes.

#### 4. Abgeleitete Anforderungen an Hardware und Software

Ideal wäre eine Physikalische Trennung der unterschiedlichen Domänen. Dies lässt sich aber im Automobil nicht erreichen, denn die Kommunikation der Infotainment Plattform mit dem Bordnetz ist eine Anforderung der Fahrzeughersteller und auch der Trend zu wenigen aber dafür mächtigeren Steuergeräten läuft dem zuwider.

Dennoch müssen die Trustdomains voneinander separiert sein. Im Falle der Angreifer aus dem Internet kann dies auch virtuell geschehen, indem die Trennung der Hardware durch Separation Kernel simuliert wird. Durch die geringe Codebasis wird hier das Risiko von Programmierfehlern reduziert. Zudem besteht hierbei die Möglichkeit einer formalen Verifizierung der korrekten Funktionsweise eines solchen Separationkernels. Pro Trustdomain wird vom Separationkernel eine Partition bereitgestellt, in der dann das auf die jeweilige Domäne zugeschnittene Betriebssystem (OS) läuft. Im Automobilen

Umfeld werden hier Windows-, Linux-(siehe [3]), Android- und Autosar-Betriebssysteme (siehe [3]) diskutiert. Die aus diesem Ansatz resultierende Architektur eines IVI Steuergeräts, z.B. eine sogenannte Head Unit, ist in der nachfolgenden Abbildung dargestellt:

### Architektur zur Umsetzung von a priori Policies

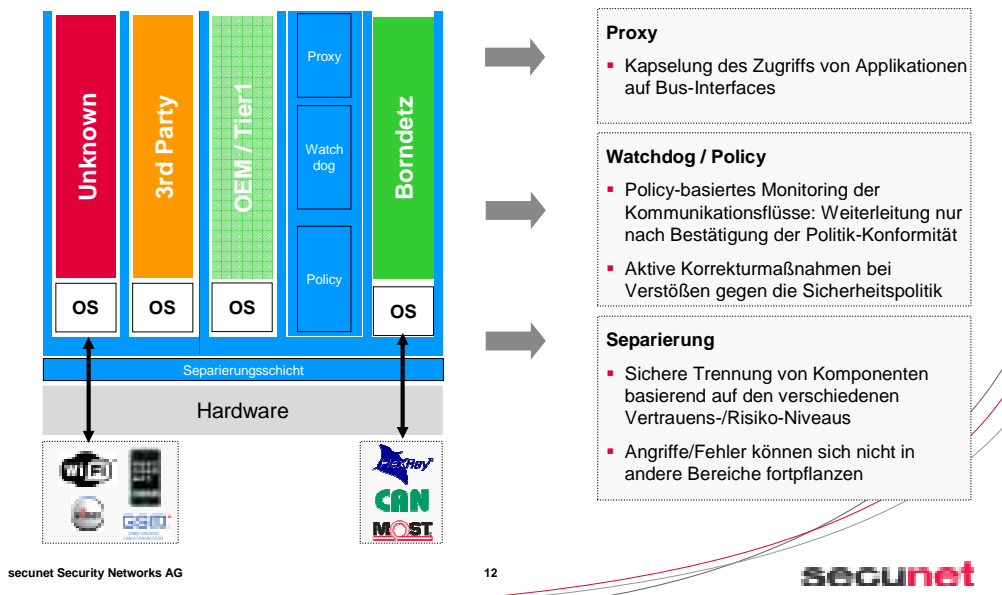


Abbildung 9: Architektur zur Umsetzung von a priori Policies

Dabei soll der Austausch von Informationen zwischen den verschiedenen Domänen nur auf den Austausch von Daten über Proxies beschränkt sein. Diese Proxies kapseln den Zugriff von Applikationen auf Bus-Interfaces. Um hier ein möglichst hohes Sicherheitsniveau zu erreichen, ist eine Unterstützung des Separationkerns durch die zugrunde liegende Hardware wünschenswert, die in Ergänzung der MMU (Memory Management Unit) für die Kontrolle des Zugriffs von Applikationen auf den RAM – Speicher eine sogenannte IOMMU bieten, die auch den Zugriff auf die Peripherie einer Infotainment Plattform, z.B. CAN Controller, bietet. Dadurch wird eine Manipulation der Kommunikationswege durch bösartige Applikationen sehr aufwendig.

Für die Kontrolle der ausgetauschten Daten sind Überwachungsinstanzen notwendig, die selbst nicht von den unbekannt nachladbaren Applikationen manipuliert werden können. Diese Überwachungsinstanzen (Watchdog) monitoren den Datenfluss und entscheiden anhand eines Regelwerks (Policy), welche Daten zur Weiterleitung freigegeben werden und welche geblockt werden müssen. Das Regelwerk setzt dabei keine Kenntnis der Applikationen voraus, die auf Bordnetze zugreifen wollen. Damit kann auch unbekannte Malware nicht auf unzulässige Weise mit dem Fahrzeug kommunizieren, z.B.

indem persönliche Daten aus dem Fahrzeug ausgelesen werden. Damit auch obiges Verfügbarkeitserfordernis abgedeckt werden kann, muss die Überwachungsinstanz auch in der Lage sein, die Quelle von erkanntem Fehlverhalten zu isolieren und nach Möglichkeit zu neutralisieren.

## **5. Referenzen**

[1] <http://www.autosec.org/pubs/cars-oakland2010.pdf>

[2] <http://www.genivi.org/>

[3] <http://www.autosar.org/>