

# **Embedded Security in Automobilen: Chancen und Risiken**

**Warum die konventionelle IT-Sicherheit für PCs im Automobil nicht funktioniert**

Dipl.-Inf. **A. Bogdanov**, escript – Embedded Security, Bochum;  
Dr.-Ing. **J. Pelzl**, escript – Embedded Security, Bochum;  
Dr.-Ing. **T. Wollinger**, escript – Embedded Security, Bochum;

## **Kurzfassung**

Die zunehmende Vernetzung von eingebetteten Systemen wird - neben dem Internet - eine weitere Revolution der IT-Technologie darstellen, die unser alltägliches Leben in einem ähnlichen Ausmaß verändern wird. Ein "eingebettetes System" liegt genau dann vor, wenn das Gerät im Wesentlichen für eine Anwendung konzipiert ist, mit "Intelligenz" (d.h. mit einem Mikroprozessor) ausgestattet ist und die Rechnerfunktionalität für den Benutzer nicht sichtbar ist. Eben solche Systeme sind im Automobil der Neuzeit verbaut. Die IT-Sicherheit nimmt in solch allgegenwärtigen Computeranwendungen wie dem Automobil eine extrem wichtige Rolle ein.

In diesem Beitrag werden verschiedene Aspekte des Themas „Embedded Security“ in einer Gesamtdarstellung betrachtet und spezifische Probleme und Lösungen werden diskutiert. Es wird herausgestellt, warum die konventionelle IT-Sicherheit im Bereich der PC-Netzwerke nicht auf den Bereich Automotive übertragbar ist. Ferner werden eine Reihe von jetzigen und zukünftigen Fragestellungen zu der IT-Security im Automobil analysiert und verschiedene Lösungsansätze aufgezeigt. Zusätzlich werden Schwierigkeiten der Embedded Security im speziellen Bereich des Automobils im Vergleich zu anderen eingebetteten Anwendungen mit Bedarf an IT-Security betrachtet. In Anbetracht derzeit existierender Sicherheitslösungen für einzelne Komponenten im Automobil, wird die Frage nach einem ganzheitlichen Ansatz für ein Sicherheitskonzept im on-board Netzwerk diskutiert.

## 1. Einleitung

In den vergangenen Jahrzehnten fand eine zunehmende Vernetzung von Computern durch das Internet statt. Anwendungen wie das World Wide Web und der E-Mail-Verkehr haben den Informationsfluss und die Kommunikation in vielen Lebensbereichen dramatisch beeinflusst. Geschäftsabläufe, private Kommunikation, Interaktion zwischen Bürgern und öffentlicher Verwaltung etc. haben nahezu revolutionäre Veränderungen erfahren. Hierdurch sind allerdings auch viele neue Sicherheitsprobleme entstanden, wie zum Beispiel Anonymität, Identitätsdiebstahl, Computerviren und Schutz digitaler Inhalte.

Heute hat bereits eine weitere Revolution der IT-Technologie begonnen, die aus der Vernetzung von eingebetteten Systemen besteht und unser alltägliches Leben in ähnlichem Ausmaß verändern wird, wie es das Internet in den letzten Jahren getan hat. Ein "eingebettetes System" liegt vor, wenn das Gerät im Wesentlichen für eine Anwendung konzipiert ist, mit "Intelligenz" (d.h. mit einem Mikroprozessor) ausgestattet ist und die Rechnerfunktionalität für den Benutzer nicht sichtbar ist (d.h. über keinen Bildschirm oder gängige Tastatur verfügt). Genau solche Systeme sind im Automobil der Neuzeit verbaut. Da vernetzte Mikrocontroller im Bereich Automotive mittlerweile allgegenwärtig sind, spricht man auch oft von Pervasive (alles durchdringend) oder Ubiquitous (allgegenwärtig) Computing. In einer solch pervasiven Computeranwendung wie dem Automobil spielt IT-Sicherheit eine extrem wichtige Rolle.

Bei dem Automobil unterscheiden wir zwei Szenarien: Auf der einen Seite stellt das Automobil selbst ein komplexes Netzwerk bereit, welches bis zu 100 Mikrocontrollern in ECUs (Electronic Control Units) durch die verschiedensten Bussysteme (wie z.B. MOST, CAN) verbindet.

Auf der anderen Seite wird zukünftig jedes Automobil Teil eines umfassenden Netzwerks sein und von Automobil zu Automobil (Car-to-Car) bzw. von Automobil zu einer Infrastruktur (Car-to-Infrastructure) mit anderen Applikationen kommunizieren.

Dieser Beitrag gliedert sich in zwei Teile: Ziel des ersten Teils ist es, verschiedene (aber sicherlich nicht alle) Aspekte des Themas Embedded Security in einer Gesamtdarstellung näher zu beleuchten und spezifische Probleme und Lösungen zu betrachten. Es wird herausgestellt, warum die konventionelle IT-Sicherheit im Bereich der PC-Netzwerke nicht auf den Bereich Automotive übertragbar ist. Hierbei wird zusammenfassend der Stand der Technik der folgenden ausgewählten Probleme betrachtet: Ressourcenbeschränkung durch kostenoptimierte Prozessoren, Reverse Engineering, Seitenkanalangriffe, beschränkte Wartungsmöglichkeiten, neue Geschäftsmodelle und Systemkomplexität.

Im zweiten Teil des Beitrags werden eine Reihe von jetzigen und zukünftigen Fragestellungen zu IT-Security im Automobil analysiert und Lösungsansätze aufgezeigt. Zusätzlich werden Schwierigkeiten der Embedded Security im Automobil im Vergleich zu anderen eingebetteten Anwendungen mit Bedarf an IT-Security betrachtet. In Anbetracht der zurzeit existierenden Sicherheitslösungen für einzelne Komponenten im Automobil wird die Frage nach einem ganzheitlichen Ansatz für ein Sicherheitskonzept im on-board Netzwerk diskutiert.

## **2. Herausforderung durch eingebettete Systeme im Automobil**

In diesem Teil werden wir auf die wesentlichen Merkmale eingebetteter Systeme eingehen und das Thema der eingebetteten Sicherheit näher betrachten. IT-Sicherheit in eingebetteten Systemen stellt spezifische Anforderungen an die Plattform und benötigt besondere Lösungsansätze, die Besonderheiten, wie die bestehende Ressourcenbeschränkung und Anderes, berücksichtigen. Im Allgemeinen kann die konventionelle IT-Sicherheit aus dem Bereich der PC-Netzwerke nicht auf eingebettete Systeme im Automobil übertragen werden, da die vorhandenen Plattformen in der Regel über unzureichende Rechenleistung verfügen. Ein weiterer Grund besteht in den verschiedenartigen Schutzzielen von Standard-PCs gegenüber eingebetteten Systemen. Während man sich bei Standard-PCs vor Software-Angriffen schützt, die z.B. über Netzwerkverbindungen durchgeführt werden können,

muss man im Bereich der Automotive Security zusätzliche Angriffsmöglichkeiten auf die Hardware berücksichtigen, da ein Angreifer in der Regel auch physikalischen Zugriff auf das Gesamtsystem Automobil hat.

## **2.1 Ressourcenbeschränkung durch kostenoptimierte**

### **Prozessoren**

Eine kostenoptimierte Realisierung ist nicht durch eine einfache Übertragung von Sicherheitstechnologien aus der PC-Welt auf das Automobil realisierbar, da im Automobil auf eingeschränkte eingebettete Rechner-Architekturen Rücksicht genommen werden muss. Die absolute Mehrheit eingebetteter Geräte verfügt nur über eingeschränkte Ressourcen, die normalerweise niedrige Rechenleistungen, begrenzte Speichermöglichkeiten und schmale Kommunikationsbandbreite einschließen. Dies ergibt sich aus der Kostenoptimierung von Mikroprozessoren im Bezug auf Hardwarefläche und Energieeffizienz.

Durch diese Faktoren wird der Einsatz gängiger Schutzlösungen wie SSL oder IPSec aus der PC-Welt ausgeschlossen. Darüber hinaus ist die Verwendung von kryptographischen Standardmechanismen in vielen eingebetteten Systemen durch die Ressourcenbeschränkung stark erschwert. Bei der Entwicklung der meisten PC-Anwendungen kann man auf unzählige Standardlösungen zurückgreifen, es bedarf keineswegs einer spezialisierten Implementierung von Kryptoalgorithmen wie AES oder RSA. Diese Standardlösungen umfassen verschiedene Open-Source Kryptobibliotheken (z.B. OpenSSL), als auch die für die Applikationen zur Verfügung stehenden kryptographischen Dienste von PC-Betriebssystemen (z.B. Cryptographic Service Providers unter Microsoft Windows). In eingebetteten Systemen existieren solche Standardmechanismen üblicherweise nicht. Der Versuch die OpenSSL-Kryptofunktionen auf einem typischen 8-Bit Prozessor zu kompilieren hat einen extrem ineffizienten Programmcode zur Folge, der in der Regel übermäßig viel Speicher (sowohl RAM als auch ROM oder Flash) benötigt und über eine äußerst niedrige Performance verfügt. Dies führt

zwangsläufig dazu, dass die erforderlichen Kryptoalgorithmen auf eingebetteten Plattformen jeder Art einzeln implementiert werden müssen, da die optimalen Methoden zur Implementierung von Kryptoalgorithmen von prozessorspezifischen Parametern abhängig sind. Für Public-Key Kryptosysteme können diese das Verhältnis der Laufzeiten von Multiplikation und Inversion in endlichen Körpern bestimmter Größe einbegreifen, was beispielsweise für die Wahl der optimalen Formeln bei der Implementierung von ECC (Elliptic Curve Cryptography) von großer Bedeutung ist. Um den Einsatz eingebetteter Plattformen in geschützten Echtzeitsystemen zu ermöglichen, werden kryptographische Algorithmen oft in Assembler und/oder in spezialisierter Hardware implementiert, was ihren Durchsatz wesentlich erhöhen kann.

## 2.2 Physikalische Angriffe

Beim Design von PC-Sicherheitssystemen wird fast immer angenommen, dass die physikalische Implementierung des PCs eine „Black Box“ für den Angreifer darstellt. Dies bedeutet, dass die Schutzmechanismen nur über logische Schnittstellen angreifbar sind. Da eingebettete Systeme häufig leicht zugänglich sind (wie es der Fall in den meisten automotiven Applikationen ist), besteht hier ein erhöhtes Schadenpotenzial bezüglich der physikalischen Angriffe (auch als „Angriffe auf Implementierungen“ bekannt). Diese sind neben den klassischen „logischen“ Angriffen, welche auch auf PC-Systeme anwendbar sind, für eingebettete Systeme charakteristisch. Bei physikalischen Angriffen wird die Implementierung als eine so genannte „Grey Box“ gesehen. Es wird zwischen den folgenden Arten von Seitenkanalangriffen unterschieden:

**Passive Angriffe:** Zu dieser Gruppe gehören Angriffe, die auf der Beobachtung eines physikalischen Parameters der Implementierung, der von der Schlüsselinformation moduliert wird, basieren. Die typischen Beispiele der passiven Angriffe sind klassische Seitenkanalangriffe wie z.B. Simple Power Analysis (SPA), Differential Power Analysis (DPA), Electromagnetic Analysis (EMA) und Timing Attacks (TA).

**Aktive nichtinvasive Angriffe:** Zu dieser Klasse gehören z.B. Angriffe, die auf der Generierung von Hardwarefehlern während der Ausführung eines Kryptoalgorithmus und ihrer darauffolgenden Analyse, basieren. Die klassischen Beispiele solcher Angriffe sind Differential Fault Analysis (DFA) und energetische Angriffe (Energy Attacks), die unter anderem Glitching (sowohl an Stromversorgung als auch an Takt) einschließen.

**Aktive invasive Angriffe:** Hier spricht man von Angriffen auf ICs, die mit einer unmittelbaren Penetration dieser einhergehen. Zu den invasiven Angriffen gehören Sondierungsangriffe (Probe Attacks), die oft mit verschiedenen Bearbeitungsmethoden (Machining Methods) kombiniert werden.

Zusätzlich sind eingebettete Systeme der erhöhten Gefahr ausgesetzt, dass die Implementierungsdetails dem Angreifer durch Reverse Engineering bekannt werden können. Um dies zu verhindern, sollten sichere eingebettete Systeme auch „tamper-resistent“ implementiert werden.

Viele von den physikalischen Angriffen sind nur von Angreifern mit mittlerem und hohem Angriffspotential durchführbar: In dem zu schützenden eingebetteten System müssen nur dann Implementierungen von Gegenmaßnahmen für komplizierte physikalische Angriffe vorliegen, wenn ein starker Angreifer wahrscheinlich ist. Die Gegenmaßnahmen können Maskierungen, zufälligen Takt, Rechnungsredundanz, spezialisierte Sensoren (Licht, Temperatur, Integrität und so weiter) umfassen.

## **2.3 Beschränkte Wartungsmöglichkeiten**

Da eingebettete Systeme oft im Feld eingesetzt werden, sind die Wartungsmöglichkeiten zumeist äußerst beschränkt. Hingegen können PC-Anwendungen fast immer durch den Systemadministrator mit beliebiger Häufigkeit gewartet werden. Im automotiven Bereich sind die Wartungsmöglichkeiten stark begrenzt und oft nur in Werkstätten möglich, die in vielen Hinsichten nicht als vertrauenswürdig angesehen werden können. Diese Tatsache hat zur Notwendigkeit, dass die verfügbaren

Wartungsmöglichkeiten schon beim Entwurf eines automotive Systems zu berücksichtigen sind.

Außerdem werden viele Komponenten eingebetteter Systeme entweder direkt in Hardware oder in ROM implementiert, wodurch das Updaten dieser Module ausgeschlossen wird. Solche Einschränkungen sind in den meisten PC-Anwendungen nicht gegeben, weil fast alle relevanten Module in der Software implementiert sind, die auf der frei beschreibbaren Festplatte abgelegt werden. Durch Updates können kritische Sicherheitsfehler behoben werden oder veraltete kryptographische Systeme ausgetauscht werden, was in vielen eingebetteten Systemen nach der Herstellung, Initialisierung und Personalisierung nicht mehr möglich ist.

## **2.4 Neue Geschäftsmodelle**

Eingebettete Sicherheit ermöglicht neue Geschäftsmodelle, welche jedoch ohne geeignete Schutzmaßnahmen nicht realisierbar wären. Eines dieser neuen Geschäftsmodelle besteht zum Beispiel in dem Freischalten von Leistungsmerkmalen, was sich z.B. nach dem Verkauf eines Automobils durchführen lässt. Mögliche Features können z.B. Kartenmaterial für Navigationsgeräte, Anpassen der Motorleistung oder erweiterte CoDecs für Multimedia-Einheiten sein. Eine solche Freischaltlösung ermöglicht zwar zahlreiche neue und innovative Geschäftsmodelle, muss jedoch technologisch sorgfältig abgesichert werden, um Missbrauch zu vermeiden und den notwendigen Umsatz sicherzustellen. Die Einführung einer Freischaltlösung bedarf sowohl technologischer Änderungen im Steuergerät als auch organisatorischer Änderungen in den Abläufen bei den Herstellern.

Ferner erlauben eingebettete Sicherheitsmechanismen Software-Updates über das Netzwerk (z.B. über GPRS) oder das Zuspielen von aktualisierten Daten. Weitere mögliche Geschäftsmodelle ergeben sich über die Auswertung des aktuellen Standortes, um beispielsweise lokale Geoinformationen für den Anwender bereitzustellen.

## 2.5 Systemkomplexität

Ein großer Teil moderner eingebetteter Systeme, dazu zählen auch zahlreiche Automobilanwendungen, bestehen aus vielen verteilten Komponenten. Heutzutage beinhalten moderne Fahrzeuge oft über 100 Steuergeräte. Jedes davon wird auf der Basis eines Mikrokontrollers implementiert. Diese Komponenten sind durch unterschiedliche Kommunikationsbusse (LIN, I<sup>2</sup>C, CAN, FlexRay, MOST, GigaStar, etc.) vernetzt. Oft sind die Steuergeräte im Auto in drei Unternetzwerke organisiert: Basisfunktionen, sekundäre Funktionen und Infotainmentfunktionen. In der Regel verfügt das Netzwerk über mehrere Schnittstellen nach außen, einige davon sind drahtlos (WLAN IEEE 802.11, 3G, Bluetooth).

Die Komplexität eines Automotive-Netzwerkes wird durch die stark ausgeprägte Heterogenität seiner Komponenten massiv erhöht. Verschiedene Steuergeräte verfügen über sehr unterschiedliche Rechenmöglichkeiten und benötigen verschiedenartige Schutzmechanismen, je nach ihrer Zweckbestimmung. Dies stellt einen weiteren Unterschied zu den PC-Systemen dar, in welchen oft nur zwischen zwei Rechnertypen (Server und Client) unterschieden wird.

Des Weiteren verfügen Automobile, sowie viele andere eingebettete Systeme, über eine komplexe Umgebung. Es gibt zahlreiche Subjekte in der Umgebung des Autos, die die Sicherheit des Fahrzeugs beeinflussen können indem sie versuchen die vom Hersteller eingeführten Sicherheitsregeln zu verletzen. Diese Subjekte in der Umgebung haben unterschiedliche Systemkenntnisse und Angriffsmöglichkeiten.

Alle diese Aspekte machen den Schutz von komplexen eingebetteten Systemen äußerst schwierig. Die Betrachtung zeigt auch, dass die Sicherheit von Automotive-Systemen, sowie von vielen weiteren komplexen eingebetteten Systemen, nur durch ein ganzheitliches, in jeder Hinsicht

durchdachtes und entwicklungsbegleitendes Sicherheitsdesign gewährleistet werden kann.

### **3. IT-Sicherheit im Automobil: Gegenwart und Zukunft**

Im zweiten Teil des Beitrags werden eine Reihe von jetzigen und zukünftigen Fragestellungen zu IT-Security im Automobil analysiert und Lösungsansätze aufgezeigt. Es werden zusätzliche Schwierigkeiten der Embedded Security im Automobil, im Vergleich zu anderen eingebetteten Anwendungen mit Bedarf an IT-Security betrachtet. In Anbetracht derzeit existierender Sicherheitslösungen für einzelne Komponenten im Automobil, wird die Frage nach einem ganzheitlichen Ansatz für ein Sicherheitskonzept im on-board Netzwerk diskutiert.

#### **3.1 Status Quo**

Momentan sind fast alle Sicherheitskomponenten im Fahrzeug von einander logisch getrennt. Das heißt, für jede Sicherheitsanwendung existieren separate Schlüsselhierarchien und Sicherheitslösungen. Typische geschützte Anwendungen im Automobil umfassen:

**Softwareupdates:** Hier wird anhand einer Signatur für die Software vom Steuergerät entschieden, ob das Update gültig ist und eingespielt werden kann. In der Regel wird der Mechanismus entweder als digitale Signatur (SigCCC) oder als Message Authentication Code (SigC) implementiert. Die Signatur/der MAC wird in jedem Fall vom OEM bzw. Zulieferer erstellt. Dabei wird die Signatur vom jedem Steuergerät einzeln verifiziert. Es existiert also kein zentrales sicheres Steuergerät, das die Updateinformationen loggen kann.

**Freischaltung:** Diese Anwendung hängt eng mit den Softwareupdates zusammen, unterscheidet sich jedoch in ihrem Ansatz. Beim sicheren Freischalten handelt es sich um das Aktivieren vorhandener Funktionalitäten gegen Gebühr im Gegensatz zum Einbringen aktualisierter Softwareversionen.

**Wegfahrsperre und Verriegelung:** Dies ist eine klassische automotiv Sicherheitsapplikation. Zur Entriegelung des Fahrzeuges, authentifiziert sich der Fahrer/der Besitzer mithilfe eines Autoschlüssels, Zum Starten des Motors ist jedoch zumeist eine separate Authentifizierung mit einem abweichenden Mechanismus erforderlich.

**Digitaler Tachograph (Lkw) und Kilometerzähler (Pkw):** Hier werden die Daten aus dem Kilometersensor ausgelesen und, im Falle des gesetzlich reglementierten digitalen Tachographens, in einer sicheren Umgebung abgelegt. Zusätzlich ist die Authentifizierung des Fahrers, gegenüber dem digitalen Tachographen, zur Aufnahme von Streckendaten notwendig. Der digitale Tachograph bietet Schnittstellen zum Ablesen der Daten durch externe Subjekte an. Der einfachere Kilometerzähler ist überwiegend in Pkw eingesetzt und wird als abgesicherter Speicher implementiert.

**Mauterhebung:** In dieser Applikation kommen schon heute kryptographisch gesicherte Verbindungen- zwischen einzelnen Modulen im Feld und dem Backend-System- massiv zum Einsatz. Außerdem sind die Mautmodule weitgehend durch physikalische Gegenmaßnahmen vor Manipulationen geschützt.

**Infotainment:** Im Infotainment-Bereich werden bereits zu heutiger Zeit komplizierte DRM-Lösungen (Digital Rights Management) zur Verwaltung von digitalem Content verwendet.

Alle diese Applikationen basieren schon heute im Wesentlichen auf solchen kryptographischen Verfahren wie digitale Signaturen, Verschlüsselung, Authentifizierungsprotokolle, PKI und so weiter. Allerdings existiert so gut wie kein Zusammenhang zwischen diesen Sicherheitsanwendungen. Dies führt dazu, dass mehrere Implementierungen derselben Kryptoalgorithmen für die Kommunikation über externe Schnittstellen in einem Fahrzeug vorliegen. Außerdem gibt es oft mehrere physikalisch abgesicherte Umgebungen zur Durchführung sicherer Berechnungen und zum sicheren Abspeichern von Daten, was unter Anderem zu der Erhöhung von Herstellungskosten für solche Komponenten führt..

Des Weiteren erfolgt die Beauftragung von Zulieferern komponentenweise, wodurch die mehrfache Verwendung der Sicherheitslösungen weiter verhindert wird. Das liegt zum Teil daran, dass unterschiedliche Abteilungen bei automotiven OEMs für unterschiedliche Sicherheitslösungen zuständig sind. Oft gibt es keinen Informationsaustausch zwischen solchen Abteilungen innerhalb eines OEMs. Dementsprechend sind Realisierungen von Sicherheitsmechanismen fast immer unabhängig voneinander.

### **3.2 Fragestellung IT-Sicherheit in Zukunft**

Fahrzeuge kommunizieren heute bereits in einem geringeren Umfang kabellos, z.B. um Online- und Diagnose-Dienste umsetzen zu können. In Zukunft wird es erforderlich sein, große Datenmengen mit dem Fahrzeug auszutauschen, selbst wenn es sich dabei außerhalb der kontrollierbaren Umgebung einer Werkstatt befindet. Dies ist notwendig um z.B. Diagnosen, Programmierungen und um Online-Dienste zur Verfügung zu stellen. Dazu werden drahtlose Schnittstellen zum Einsatz kommen, wie z.B. WLAN, GPRS, UMTS, Car-2-Infrastructure oder Car-2-Car. Der Zugriff auf das Fahrzeug ist dann nicht mehr in dem Maße kontrollierbar, wie vergleichsweise der Anschluss des Diagnosegerätes in einer Werkstatt.

Neben den in Zukunft entstehenden neuen Herausforderungen an die Sicherheit, um z.B. die genannten neuen Schnittstellen abzusichern, ist es unumgänglich, die aktuellen und zukünftigen Sicherheitsmaßnahmen immer wieder auf Ihre Wirksamkeit zu prüfen. Zusätzlich müssen Lösungen für derzeit bestehende Probleme gefunden werden; es existieren immer noch sicherheitstechnische Insellösungen zur Absicherung hoch sensibler Daten (z.B. Kilometerstand, Wegfahrsperre), welche bislang durch die jeweiligen Projekte separat abgesichert werden müssen. Im Sinne einer ganzheitlichen Strategie für die kommenden Fahrzeuggenerationen ist es daher ratsam, dass die Anforderungen gesammelt, kanalisiert und zu einer übergreifenden Sicherheits-Architektur für das Fahrzeug entwickelt werden.

### **3.3 Existierende Lösungsansätze**

In den letzten Jahren haben immer mehr IT-Sicherheitslösungen Einzug in das Automobil gehalten. Dabei haben sich separate Sicherheitslösungen für einzelne Komponenten - wie z.B. für die Wegfahrsperrung, das sichere Flashen oder die Funktionsfreischaltung - entwickelt, welche unabhängig voneinander entworfen und implementiert werden. Diese historisch gewachsenen Insellösungen funktionieren zwar in der Regel, haben jedoch einige gravierende Nachteile gegenüber einer ganzheitlichen Sicherheitslösung:

Die Implementierungen nutzen Überschneidungen in der Sicherheitsarchitektur nicht aus. Hierdurch entstehen Mehrkosten, die durch die Mehrfachentwicklung einzelner Komponenten bedingt sind.

Die Schutzziele sind nicht vereinheitlicht, d.h. es gibt unterschiedliche Ausprägungen von Sicherheit in den einzelnen Komponenten. Gegebenenfalls können sogar funktional identische Komponenten unterschiedliche Sicherheitsfeatures aufweisen.

Ein Gesamtsystem ist immer genau so sicher wie die schwächste Komponente. Das heißt das schwächste Glied in der Kette bestimmt die Sicherheit des ganzen Systems.

Ziel einer ganzheitlichen Sicherheitsarchitektur ist es daher, unter Berücksichtigung der oben genannten Punkte, sinnvolle Schutzmaßnahmen zu definieren.

### **3.4 Zukünftiger ganzheitlicher Lösungsansatz**

Ausreichende IT-Sicherheit für den Bereich Automotive ist langfristig nur durch ein übergreifendes Sicherheitskonzept realisierbar. Hierbei muss in der Regel auf die bestehenden Prozesse aufgebaut werden, um eine möglichst kosteneffektive und realisierbare Lösung zu finden. Die Veränderung

bestehender Prozesse ist aus betriebswirtschaftlicher Perspektive nicht erwünscht.

Für eine kurzfristige Verbesserung der IT-Sicherheit im Automobil, liegt in diesem Zusammenhang der praktikabelste und einfachste Weg in der Absicherung einzelner Komponenten, die in der Regel schon besteht. Langfristig führen diese Insellösungen aber nur dann zu einem sichereren Gesamtsystem, wenn durch die Automotive Security alle sicherheitsrelevanten Probleme zentral adressiert werden. Sicherheitsproblematiken nicht zentral zu lösen, ist auf lange Sicht unwirtschaftlich, da jeder Teilbereich seine Sicherheitslösung kontinuierlich einzeln neu evaluieren und verbessern muss. Die zentrale Konzeption und Verwaltung aller Sicherheitslösungen ist daher übersichtlicher und auch wirtschaftlicher, wenn Verbesserungen in das Gesamtsystem einfließen. Grundsätzlich ist ein System nur genau so sicher, wie seine schwächste Komponente, wobei besonderer Wert auf die Definition der zu schützenden Informationen und Prozesse gelegt werden muss. Um das schwächste Glied einer Kette identifizieren zu können, wird ein Gesamtüberblick des Systems benötigt. Dieser Gesamtüberblick ermöglicht dann die Analyse und die Verbesserung der existierenden Schwachstellen.,. Eine Analyse des Ist- Zustands daher in sofern sinnvoll, als das sie die Maßnahmen aufzeigt, die kurzfristig und langfristig ergriffen werden sollten um das Sicherheitslevel zu erhöhen.

Als ein besonders kritischer Bereich sei beispielhaft das Schlüsselmanagement genannt. Die Realisierung eines Schlüsselkonzeptes ist eine Aufgabe, welche die gesamte IT-Sicherheit im Automobil berücksichtigen sollte. Die Koexistenz von mehreren (verschiedenen) Schlüsselhierarchien ist zu vermeiden und eine einheitliche Schlüssel-Architektur mit wohldefinierten Rollen ist zu bevorzugen.

Generell sollte es das Ziel sein, einen pragmatischen Ansatz zu verfolgen, um kurzfristig und kosteneffizient die IT-Sicherheit im Bereich Automotive zu verbessern. Hierzu müssen die zugrunde liegenden Ressourcen im Automobil

optimal genutzt werden. Der Fokus liegt hierbei auf einem ganzheitlichen Ansatz, um Insellösungen langfristig in eine betriebswirtschaftlich sinnvolle IT-Sicherheitslösung umzusetzen.

Adressiert man mit einem umfassenden Konzept alle Sicherheitsprobleme im Fahrzeug, ist es leichter ein Gesamtsystem zu analysieren, Änderungen einzubringen und Anpassungen an aktuelle technische Entwicklungen vorzunehmen. Außerdem ist es möglich, die Schwachstellen eines Systems zu erkennen und angemessen darauf zu reagieren.

Abbildung 1 illustriert das Prinzip anhand einer Common-Criteria-orientierten Vorgehensweise [3]:

- Identifikation von Angriffspfaden auf Use-Cases: Es werden mögliche Angriffspfade auf die Use-Cases erarbeitet.
- Identifikation von Schutzzielen: Um einen Schutz vor den jeweiligen Angriffen zu erhalten, werden Schutzziele für die Use-Cases definiert.
- Bewertung von Schutzzielen: Für die einzelnen Angriffspfade wird das jeweilige Angreiferpotential bestimmt. Hierbei sollten sinnvolle, den Umständen entsprechende, Angriffsszenarien als Grundlage dienen. Nach CC wird das Angreiferpotential in die Stufen basic, enhanced basic, moderate, high und beyond high unterteilt. In einem ganzheitlichen Ansatz bietet diese Aufteilung eine umfassende Bewertung der gesamten Architektur. Die Sicherheit von verschiedenen Komponenten wird hierbei relativ zueinander betrachtet.
- Bestimmung der Maßnahmen (M1...Mn): Als Schutz vor den zuvor genannten Angriffen und zur Realisierung des Schutzzieles werden Maßnahmen definiert.
- Synergien identifizieren: In einem ganzheitlichen Ansatz besteht nun die Möglichkeit, mit einer Maßnahme gleich verschiedenen Schutzzielen zu dienen. Dies bringt den Vorteil mit sich, dass Maßnahmen wieder verwendet werden können.

## Angreiferpotential (nach CC)

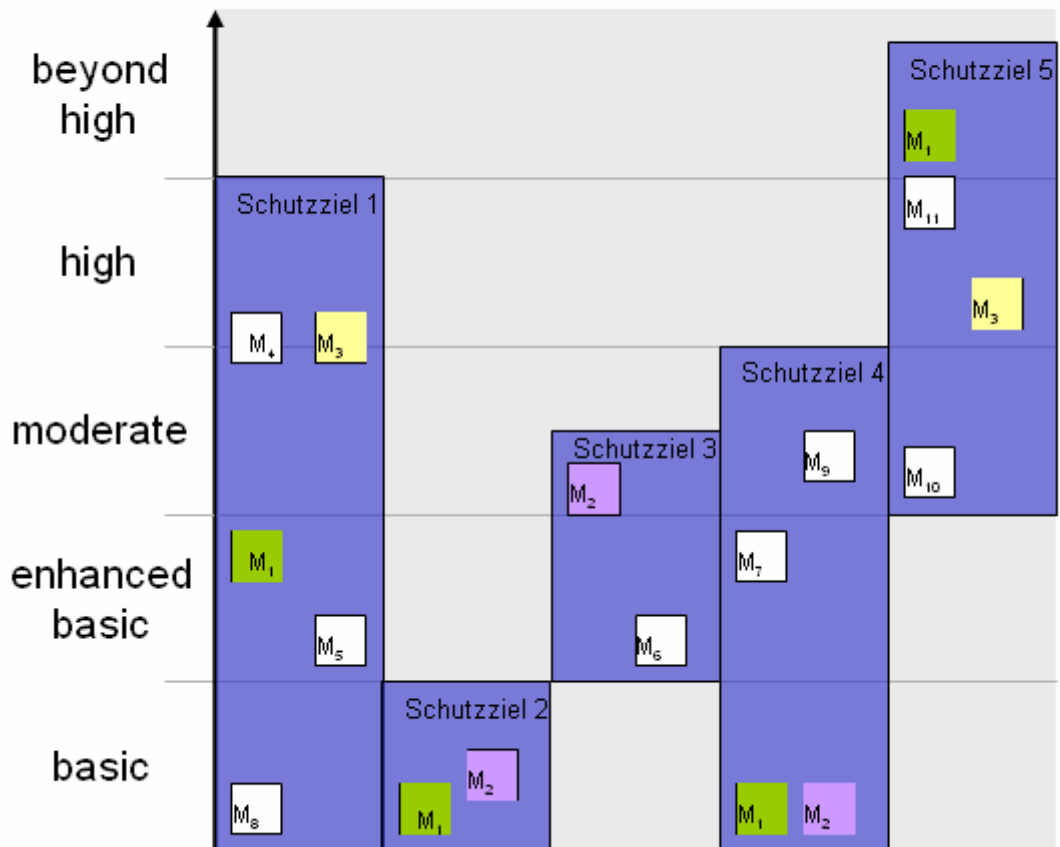


Abbildung 1: Einordnung verschiedener Schutzziele nach Angreiferpotential

Abbildung 2 zeigt das weitere Vorgehen in einem ganzheitlichen Ansatz. Nachdem (theoretisch) festgehalten wurde, welche Maßnahmen zur Realisierung der einzelnen Schutzziele verwendet werden können, werden nun die Maßnahmen realisiert. Aus Kostengründen werden in der Praxis Maßnahmen sukzessiv erarbeitet. Das heißt es werden Prioritäten festgelegt, welche Schutzziele (und damit welche Use-Cases) als erstes abgedeckt werden sollen (z.B. EWS).

Bei der Implementierung der einzelnen Schutzziele empfiehlt sich folgendes Vorgehen:

- Erfassen von Abhängigkeiten: Es wird analysiert, welche Maßnahme besonders häufig verwendet werden kann.
- Abarbeiten der Maßnahmen nach Priorität: Oft können mit wenigen Maßnahmen viele Schutzziele gleichzeitig erreicht werden. Solche Maßnahmen sind zu bevorzugen. (Siehe farbliche Kennzeichnung in den Abbildungen 1 und 2)
- Auswirkung auf Gesamtsicherheit: Die Reihenfolge der Implementierung der Maßnahmen sollte so gewählt werden, dass jede zusätzliche Maßnahme eine Steigerung der Gesamtsicherheit bedeutet. So ist es z.B. weniger sinnvoll, Schutz vor einem komplexen Angriff zu realisieren, wenn dem Angreifer wesentlich einfachere Wege offen stehen.
- Iteratives Vorgehen: Wiederholung des Vorgehens, bis alle Maßnahmen implementiert sind. (Roter Balken geht stetig nach oben.)

Ein ganzheitlicher Ansatz bietet also Vorteile in Form von Kosteneinsparung durch Synergieeffekte (mehrfache Nutzung bereits erarbeiteter Primitive) und stellt zudem eine wirksame Steigerung der Gesamtsicherheit dar. Durch identische Vorgaben und Metriken für alle Komponenten, wird eine gleichwertige und ganzheitliche Betrachtung der Sicherheit ermöglicht.

## Angreiferpotential (nach CC)

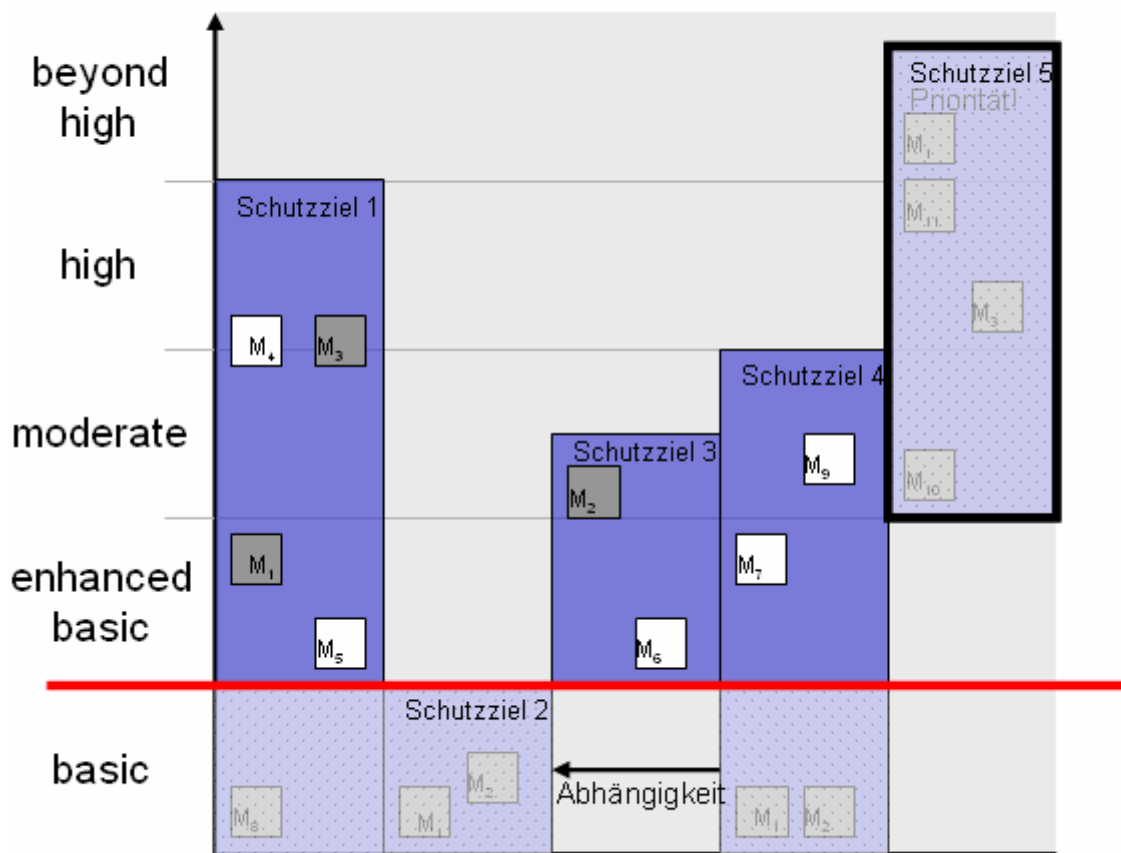


Abbildung 2: Sinnvolles Vorgehen zur stetigen Steigerung der Gesamtsicherheit

## Referenzen:

- [1] *Security Modules for Vehicles*. escrypt Whitepaper.  
<http://www.escrypt.com>
- [2] *Eingebettete Sicherheit: State-of-the-art*. Christof Paar, Jan Pelzl, Kai Schramm, André Weimerskirch und Thomas Wollinger.  
<http://www.escrypt.com>
- [3] *Common Criteria for Information Technology Security Evaluation*  
*Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit*  
*von Informationstechnik) v3.1*, Bundesamt für Sicherheit in der  
Informationstechnik, <http://www.bsi.bund.de/cc/>