



Der digitale Goldesel

Mehr Motorleistung an der Software-Tankstelle laden? In Kürze möglich. Vorausgesetzt, die im Automobil verfügbare Software hält den hohen Anforderungen an die Sicherheit stand. Mit dem Digital Rights Management kommt eine ‚Killer-Applikation‘ für Software ins Fahrzeug, die neue Geschäftsmodelle verspricht.

Zum Schutz digitaler Inhalte entwickelt sich die Technologie des Digital Rights Management (DRM) derzeit rapide – nicht nur im PC-Bereich. Besonders der Automobilbranche bietet das Verfahren eine Fülle neuer Möglichkeiten. Es scheint sogar, als entwickelt sich DRM als die ‚Killer-Applikation‘ für die nächste Generation von IT-Systemen im Automobil.

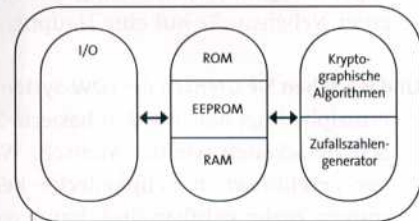
Das digitale Rechte-Management erlaubt dem Inhaber digitaler Inhalte, seine Rechte zu wahren und in einer wohl definierten Form durchzusetzen. Vor allem in den Fällen, in denen die digitalen Inhalte bei dem Benutzer vollständig vorliegen müssen.

Für die Automobilbranche wird dies in Zukunft von großem Interes-

se sein. Bereits heute werden mehr als 50 Prozent aller neuen Minivans in den USA mit einem Multimediapaket, inklusive Bildschirmen für die Rücksitze, ausgestattet.

Dies ist jedoch erst der Beginn digitaler Absicherung softwarebasierter Inhalte im Fahrzeug. Sehr viele innovative Anwendungen und neue Geschäftsmodelle werden folgen. Diese basieren dabei im Wesentlichen auf folgenden vier prinzipiellen Ideen:

- Zeitbefristete Nutzung, beispielsweise können Navigationsrouten nur zwei Wochen lang genutzt werden,
- mengenbefristete Nutzung, ein Videofilm kann nur dreimal abgespielt werden,



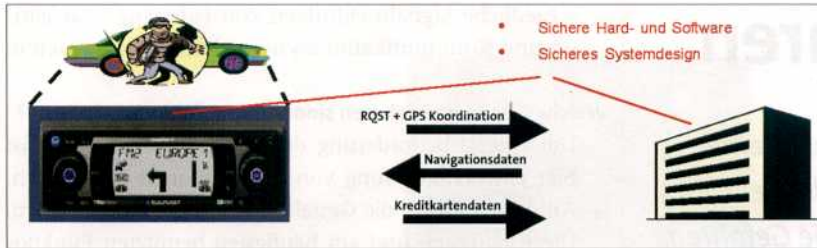
Mehr Leistung und ein Sportfahrwerk-Gefühl an der Tankstelle aufspielen: Software wird in Kürze zum Tunen eingesetzt. Mit dem Digitalen Rechte Management ist dies auch sicher. Bild: BMW Group

- an ein Gerät gebundene Nutzung, zum Beispiel kann eine Flash-Software zum Motor-Tuning nur auf einem bestimmten Fahrzeug installiert werden,
- nachträgliche Aktivierung, beispielsweise können von Werk aus verbaute Zusatzkomponenten nachträglich aktiviert werden.

Darüber hinaus sind alle wohl definierten Regeln und Kombinationen vorstellbar. Unter anderem kann ei-

DRN schützt vor illegalen Intentionen des Benutzers

ne nachträglich aktivierte Komponente wie ein Navigationssystem genau drei Wochen lang bei maximal zehn Routenführungen genutzt werden oder ein Motor-Update verbleibt nur für fünf Tage in der Steuereinheit. Vor allem aber können diese Regeln mit Hilfe einer DRM-Lösung gegen die (illegalen) Intentionen des Benutzers durchgesetzt werden.



Navigationsdaten auf Abruf: Ein Autofahrer fordert von dem Dienstanbieter die Daten an und bezahlt diese. Wegen der potentiellen Bedrohungen ist ein sicheres Systemdesign nötig.

Eng verbunden mit den genannten Geschäftsmodellen ist die Möglichkeit des sicheren Flashens von Software im Automobil. Wesentliche Voraussetzung dafür ist, dass ein Benutzer das Recht zur Benutzung erwerben muss und eine illegale Nutzung verhindert wird. Die Vergangenheit lehrt jedoch, dass dies nicht immer glückt. Prominenter Fall: der Pay-TV Sender Premiere.

Ein sorgfältig umgesetztes DRM ist somit die Grundlage eines solchen Geschäftsmodells. Denn die Möglichkeit das DRM System zu umgehen, untergräbt das Geschäftsmodell und kann zu einem Komplettverlust des Anbieters führen. Erst Verschlüsselungsalgorithmen und Zugangsbeschränkungen bringen die benötigte Sicherheit.

Für viele Anwendungen, insbesondere wenn keine großen Werte geschützt werden, können somit praktikable Lösungen aufgebaut werden. Eine Gefahr für DRM im Fahrzeug sind allerdings physikalische Angriffe. Der Benutzer beziehungs-

weise das Wartungspersonal des Automobils hat nahezu beliebigen Zugang zu allen Komponenten. Ein Angreifer kann daher versuchen die Software des Bordcomputers (Head Unit, Infotainment-Einheit et cetera) oder des Steuergerätes auszulesen oder zu verändern.

Ein anderer Ansatz sind so genannte Seitenkanalattacken, bei denen das Schlüsselmaterial durch die Beobachtung des Stromverbrauchs und des Laufzeitverhaltens des Steuergerätes ermittelt wird. In beiden Fällen kann danach Missbrauch getrieben werden, so dass die Geschäftsmodelle kollabieren.

Um ein wirklich sicheres DRM-System zu erhalten, das solche Angriffe vereitelt, ist eine so genannte Trusted Computing (TC) Lösung er-

Geschäfte mit Software

Sobald Verfahren zur Absicherung von Software-Systemen im Automobil Einzug halten, werden in Kürze neue Geschäftsmodelle entstehen. Dann lassen sich Fahrzeuge per Mausklick seinen Vorlieben anpassen.

- Navigationsdienste on-demand
- zusätzliche Motorleistung von 20 PS für ein Wochenende
- spezielle Tuning Einstellungen on-demand
- Zukauf einer Einparkhilfe durch eine Softwareaktivierung
- beliebige Pay-per-use Dienste

nen wie die Hash-Funktion (SHA -1) und Verschlüsselungsverfahren wie AES oder Triple-DES zum Einsatz.

Diese Komponenten sind im Trusted Platform Module (TPM) vereinigt, das den sicheren vertrauenswürdigen Hardware-Kern darstellt, auf dem das TC basiert. Das TPM kommuniziert über ein Input/Output-Interface mit der Bridge des Hosts, einem PC oder einem eingebetteten Gerät, um alle Aufgaben zu erfüllen.

Manipulationssichere Software für das Automobil wird den Markt für neue Anwendungen puschen

forderlich. Dabei wird ein Hardware-Sicherheitsmodul eingesetzt, welches das kritische Schlüsselmaterial enthält und kryptographische Funktionen ausführen kann.

Das DRM wird nun mit Hilfe der TC Plattform umgesetzt, so dass eine illegale Nutzung der digitalen Inhalte nur möglich ist, wenn das Sicherheitsmodul kompromittiert wird. Dies ist allerdings nicht oder nur mit extrem hohem Aufwand möglich.

Das TC-Modul besteht aus wenigen Kernkomponenten, die manipulationssicher in Hardware realisiert werden müssen. Dazu gehören unter anderem Zufallsgenerator, Timer, nicht-flüchtiger Speicher und Asymmetrische Krypto-Algorithmen. Diese enthalten beispielsweise elliptische Kurven, RSA oder hyperelliptische Kurven. Darüber hinaus kommen Symmetrische Krypto-Funktio-

Zusätzlich wird aber auch ein sicheres Betriebssystem benötigt. Zum Beispiel kann ein TC-Software-Layer mit Sicherheitsfunktionen zwischen der TC-Hardware und dem eigentlichen Betriebssystem implementiert werden. Prominentes Beispiel für eine solche Betriebssystemerweiterung ist ‚Perseus‘, welches auch für eingebettete Anwendungen geeignet ist.

Im Automobil bietet es sich an, dass der TC-Software-Layer und das sichere Betriebssystem in den Bordcomputer integriert werden. Dadurch kann diese Einheit als vertrauenswürdiger ‚Anker‘ dienen, von dem sicherheitsrelevanten Dienste im Fahrzeug aus initiiert werden.

Autoren: Dr.-Ing. André Weimerskirch und Prof. Dr.-Ing. Christof Paar. Beide Dept. of Electr. Eng. & Information Sciences der Ruhr-University Bochum.

Sicherheitsinitiative TCG

Im Zusammenhang mit dem Digital Right Management gilt die Trusted Computing Group als wichtiger Treiber der Technologie. Die TCG ist eine Industriegruppe, der Unternehmen wie AMD, Hewlett-Packard, IBM, Intel Corporation, Microsoft, Sony und Sun Microsystems angehören.

Das TCG – früher TCPA, Trusted Computer Platform Alliance genannt – beschreibt das Gesamtsystem zur Erstellung einer Trusted Computing Hardware Plattform, bestehend aus Hardware- und Softwarekomponenten. TCG ist der notwendige Unterbau, um sichere DRM-Anwendungen zu realisieren.