Digital Rights Management Systeme (DRMS) als *Enabling Technology* im Automobil

Marko Wolf, André Weimerskirch, Christof Paar
escrypt GmbH, Bochum
{mwolf, aweimerskirch, cpaar}@escrypt.com

Abstrakt: Mit dem Einzug moderner Multimedia- und Computertechnik im Automobilbereich werden eine Vielzahl neuer Möglichkeiten aber auch Risiken durch die Verwendung geschützter digitaler Inhalte im Automobil zur Realität. Die Umsetzung von Digital Rights Management Systemen (DRMS) im Automobil ist daher nicht nur eine notwendige, sondern auch eine viel versprechende Herausforderung.

1 Digital Rights Management Systeme (DRMS)

Während Mechanismen zum Kopierschutz physikalisch oder logisch allein die illegale Vervielfältigung zu verhindern suchen, erlauben DRMS dem Rechteinhaber digitaler Inhalte (Musik, Filme, ortsbezogene Informationen, Software, ...) ein definiertes Rechtemodell gegenüber dem Rechteverwerter durchzusetzen. Neben der klassischen Pauschalverwertung sind so auch kombinierbare Modelle zur zeitbefristeten, mengenbefristeten, gerätegebundenen oder gebrauchsorientierten Verwertung möglich. Ein Rechtemodell besteht nach [St97] aus den Wiedergaberechten (z.B. Ansehen, Anhören, Drucken), Transportrechten (z.B. Kopieren, Weitergeben, Vermieten), Derivativrechten (z.B. Extrahieren, Editieren, Einbinden) und den Dienstrechten (z.B. Sicherung, Caching, Integritätssicherung). Jedes Recht einer Rechtegruppe kann wiederum mit Attributen zur Vergütung (z.B. Geld, Registrierung), zur Abgrenzung (z.B. Dauer, Anzahl, Ort) und zur Benutzergruppe (z.B. Besitzer, Fahrer) versehen werden. Ein DRMS besteht nach [RTM02] im Wesentlichen aus einem Inhalteserver und dem Lizenzserver auf Anbieterseite sowie den zugehörigen, lokal abgesicherten DRM-kompatiblen Wiedergabeprogrammen auf Nutzerseite.

2 Anforderungen an DRMS im Automobil

Im Vergleich zum klassischen Einsatzgebiet im PC-Bereich, ergeben sich für DRMS in Fahrzeugen teilweise deutlich Einschränkungen und besondere Anforderungen.

Physikalische Umgebung: Im Automobilbereich müssen sämtliche verbauten Systeme große Temperaturschwankungen, dauerhaft hohe Feuchtigkeit sowie die erhöhten mechanischen Belastungen über den gesamten Produktlebenszyklus bei minimalen Wartungs-

aufwand nahezu störungsfrei bewältigen. Dies ist eine besondere Herausforderung an alle zu verwendenden Hardwaremodule, nicht nur im Bereich von DRMS.

Eingebettete Systeme: Die Rechenkapazität und damit einhergehend die Komplexität und der mögliche Umfang der zu verwendenden Software ist im Automobilbereich nicht mit der PC-Welt zu vergleichen. Es ergeben sich daher besonders hohe Anforderungen an Laufzeiteffizienz und Speicherbedarf. Zudem ist mit vielen architekturspezifischen Einschränkungen zu rechnen.

Externe Kommunikation: Fahrzeuge verfügen in der Regel nur über begrenzte externe Kommunikationsmöglichkeiten, um sich bspw. mit einem Lizenzserver zu verbinden, neue Software zu installieren oder Schlüssel zu aktualisieren. Automobile DRMS müssen daher mit einem in Umfang und Häufigkeit äußerst geringen externen Kommunikationsbedarf nahezu vollständig automatisiert funktionieren. Zudem darf die Funktionalität des DRMS auch während einer über einen längeren Zeitraum fehlenden Möglichkeit zur externen Kommunikation nicht wesentlich beeinträchtigt werden.

Benutzerschnittstelle und Nutzbarkeit: Während ein PC-Benutzer ergonomische Ein- und Ausgabegeräte benutzen kann, müssen automobile Benutzer ihre Anwendungen über nur begrenzt ergonomische Peripherie bedienen. Zudem kann und darf von automobilen Benutzern nicht erwartet werden, über ein absolutes Minimum hinaus, in die Abläufe eines DRMS eingreifen zu müssen. DRMS müssen im Fahrzeug folglich weitestgehend autonom agieren. Sind unverzichtbare Benutzerinteraktionen notwendig, sollte der Umfang und die Komplexität der erforderlichen Ein- und Ausgabedaten so beschränkt werden, dass diese im automobilen Kontext (10er-Tastatur, Kleinbildschirm, ...) schnell und problemlos zu verarbeiten sind.

Infrastruktur/Interoperabilität: Die für DRMS notwendige, einzurichtende Schlüssel- und Zertifikatsinfrastruktur ist im automobilen Bereich eine besondere Herausforderung. Durch die Vielzahl der im Produktlebenszyklus agierenden Parteien (Hersteller, Zulieferer, OEM, Kunde, Werkstatt, Inhalteanbieter, ...) sind komplexe, zuverlässige organisatorische Strukturen notwendig. Ein weiterer wesentlicher Schlüsselpunkt ist die Interoperabilität zu bereits bestehenden DRMS, um den Kunden eine möglichste umfassende Integration ihrer bereits bestehenden digitalen Medien zu ermöglichen.

Wartung und Zuverlässigkeit: Da Fahrzeuge in der Regel nur über eine begrenzte Möglichkeit zur Wartung ihrer Software verfügen, sind Kompatibilität, Zuverlässigkeit und Wartungsfreiheit für alle automobilen Softwaremodule dringende Voraussetzung. Insbesondere ist die Sicherstellung der Wartungsfähigkeit durch die Verfügbarkeit aller notwendigen Soft- und Hardwarewerkzeuge über den gesamten Produktlebenszyklus eines Fahrzeugs unerlässlich.

Sicherheit: Neben Angriffen auf mögliche Designschwächen eines DRMS sind physikalische Angriffe auf Fahrzeugkomponenten eine besondere Gefahr für den Betreiber eines automobilen DRMS. Der Fahrzeugbesitzer bzw. das Wartungspersonal des Automobils haben nahezu beliebigen Zugang zu allen Komponenten eines Fahrzeugs. Ein Angreifer kann daher versuchen, gezielt verschiedene Daten zu manipulieren, unautorisiert Software aufzuspielen oder die hardwareseitigen Schutzmechanismen zu umgehen. Der Nutzer eines DRMS muss wiederum stets in der Lage sein, selbst zu entscheiden welche Informationen

(Personalien, Nutzungsprofile, ...) bzw. unter welchen Bedingungen er diese preisgibt. Die Vertraulichkeit gegenüber unbeteiligten Dritten ist grundsätzlich zu gewährleisten. Ferner sind geeignete Methoden zur zuverlässigen, langzeitfähigen Datensicherung und sicheren Datenübertragung (z.B. im Falle eines Fahrzeugwechsels) zu implementieren.

3 Realisierung automobiler DRMS

Um ein zuverlässiges DRMS zu erhalten, ist eine so genannte Trusted Computing (TC) Lösung erforderlich. Dabei wird ein Hardware-Sicherheitsmodul (Trusted Plattform Module, kurz TPM) eingesetzt, das das kritische Schlüsselmaterial schützt und verschiedene kryptographische Funktionen vertrauenswürdig ausführen kann sowie über einen echten physikalischen Zufallsgenerator verfügt. Ein TPM ist zudem besonders gegen unbefugte Manipulationen geschützt (siehe [KK99]) und kann nicht bzw. nur mit extrem hohem Aufwand kompromittiert werden. Das mit dem zentralen Bordrechner verbundene TPM ermöglicht, ein auf die TPM-Funktionalität basierendes, sicheres Betriebssystem bzw. eine vertrauenswürdige Softwareschicht, welche als Plattform für das eigentliche (potenziell nicht vertrauenswürdige) Betriebssystem dient. Ein prominentes Beispiel für eine solche sichere Betriebssystemplattform ist PERSEUS [PER04], welches auch für eingebettete Systeme geeignet ist. Der so gewonnene vertrauenswürdiger „Anker“ initiiert alle sicherheitsrelevanten Dienste im Fahrzeug und kann so das DRMS im gesamten Fahrzeug durchsetzen. Um den vorgenannten Anforderungen an automobile DRMS gerecht zu werden, sind nachfolgende Maßnahmen möglich.

Physikalische Umgebung: Die Mehrzahl der für ein DRMS notwendigen Komponenten sind oftmals auch schon für andere automobile Anwendungen erforderlich und entsprechen daher bereits den besonderen physikalischen Anforderungen im Automobilbereich. Für neue oder gänzlich DRMS-spezifische Komponenten können das bereits vorhandene Know-How, die Technologien und Vorkehrungen weitgehend analog angewandt werden. Ein TPM für den Einsatz in eingebetteten Systemen ist heute auch bereits verfügbar.

Eingebettete Systeme: Unsere Erfahrung zeigt, dass auch rechen- und speicherintensive kryptographische Verfahren und Sicherheitsmechanismen in beschränkten Umgebungen realisiert werden können. Viele können oft schon auf Mikroprozessoren herkömmlicher 8-Bit Steuergeräte bei minimalen Speicherbedarf umgesetzt werden.

Externe Kommunikation: Wird auf den dynamischen Lizenzerwerb weitestgehend verzichtet, wird die externe Kommunikation nur noch beim Einspielen noch unlizenzierter Software oder Medien benötigt. Die, zumindest in Europa nahezu flächendeckende, Mobilfunk-Versorgung, ist jedoch schon jetzt ausreichend um nahezu alle automobilen Geschäftsmodelle mit geschützten Inhalten zu realisieren. Der zukünftige UMTS-Mobilfunkstandard wird die Möglichkeiten eines automobilen DRMS noch weiter vervielfachen.

Benutzerschnittstelle und Nutzbarkeit: Durch den weitgehend festgelegten Verwendungskontext und einer meist gerätegebundenen Identität sind nahezu autonom agierende DRMS relativ leicht zu realisieren. Die wenigen noch notwendigen Ein- und Ausgaben können über die bereits erprobten Ein- und Ausgabegeräte der heute schon gebräuchlichen

Fahrzeugnavigation erfolgen.

Infrastruktur/Interoperabilität: Die Infrastruktur zum Lizenz- und Schlüsselmanagement muss durch den Automobilhersteller selbst oder einen externen Dienstleister bereitgestellt werden. Für den großen, weltweiten Erfolg von DRMS (im Automobil- wie auch im PC-Bereich) bleibt jedoch die Einigung auf gemeinsame Hard- und Softwarestandards für alle Parteien eines DRMS eine der, wenn nicht sogar *die* größte Herausforderung.

Wartung und Zuverlässigkeit: Die erhöhten Anforderungen an Kompatibilität, Zuverlässigkeit und Wartungsfreiheit eines automobilen DRMS lassen sich durch eine Vielzahl bewährter Methoden des Softwarequalitätsmanagements und der Softwareverifikation, wie für andere automobile Software auch, hinreichend zuverlässig sicherstellen. Die, im Vergleich zu herkömmlicher Automobilsoftware, stetige, wesentlich schneller fortschreitende Weiterentwicklung lässt sich jedoch nur durch zusätzliche Vorsorge (große Schlüssellänge, Rückfallsysteme, ...) und gelegentliche Softwareaktualisierungen beherrschen. Die Sicherstellung der Wartungsfähigkeit durch die Verfügbarkeit aller notwendigen Soft- und Hardwarewerkzeuge ist ohnehin im Rahmen der für Fahrzeuge typischen, vertraglich zugesicherten Funktionsgarantie über den gesamten Produktlebenszyklus bindend.

Sicherheit: Basiert die Sicherheit des DRMS allein auf dem TPM übersteigt eine zerstörungsfreie Manipulation die technischen und finanziellen Möglichkeiten der meisten Angreifer sowie den zu erwartenden Nutzen um ein Vielfaches. Die Privatsphäre des Benutzers lässt sich softwareseitig durch eine Reihe anerkannter kryptographischer Mechanismen relativ problemlos absichern. Notwendige persönliche Daten sind nur nach einer expliziten Freigabe allein für berechtigte Parteien sichtbar. Die langzeitfähige Datensicherung und Lizenzübertragung lässt sich mit geeignet abgesicherten Smartcards realisieren.

4 Zusammenfassung und Ausblick

DRMS im Automobilbereich sind eine *Enabling Technology* für etliche neue Geschäftsmodelle und schützen zugleich wichtige Fahrzeugkomponenten zuverlässig vor unbefugten Manipulationen. Obwohl für den erfolgreichen Einsatz von DRMS im Automobil noch einige Hürden zu meistern sind, erwarten wir schon in kurzer Zeit die Umsetzung erster DRMS im automobilen Kontext.

Literatur

[KK99] O. Kömmerling, M. Kuhn. Design Principles for Tamper-Resistant Smartcard Processors. In *USENIX Workshop on Smartcard Technology proceedings, Chicago, USA, 1999*.

[PER04] Perseus OS. Website, 2004. `www.perseus-os.org`.

[RTM02] B. Rosenblatt, B. Trippe, S. Mooney. Digital Rights Management. In *M&T Books, New York, USA, 2002*.

[St97] M. Stefik. Letting Loose the Light: Igniting Commerce in Electronic Publication. In *Internet Dreams, Mark Stefik ed., MIT Press, USA, 1997*.